Farm Credit Administration

1501 Farm Credit Drive
McLean, Virginia 22102-5090
(703) 883-4000

INFORMATIONAL MEMORANDUM

June 27, 2017

To: Chair, Board of Directors
Chief Executive Officer
All Farm Credit System Institutions

From: Samuel R. Coleman
Director and Chief Examiner

Subject: Reporting Security Incidents and Business Continuity Events to FCA

This Informational Memorandum provides Farm Credit System (System) institutions with further guidance on reporting security incidents and business continuity events to the Farm Credit Administration (FCA). The frequency of security events[1] is growing rapidly. As such, a sound and proactive internal control environment is required to monitor threats and mitigate risks. Information security promotes the banking industry-wide objectives of confidentiality, integrity, availability, and accountability of information systems, and is essential to the overall safety and soundness of an institution. System institutions' boards and management are responsible for ensuring safe and sound operations in accordance with laws and regulations.

Sound business practices emphasize that the best defense for managing cyber incidents is to implement an effective incident response plan and an information security awareness training program. Management should maintain an incident response program that includes policies and procedures for monitoring, assessing, and mitigating damage and losses from events that occur. The incident response program should include processes for containing the incident, coordinating with law enforcement and third parties, restoring systems, preserving data and evidence, assisting customers, and facilitating operational resilience of the institution.[2] Management should also establish appropriate protocols for notifying FCA of a security breach[3] and any disruption in operations that results in the activation of the institution's business continuity plan.

FCA must be notified when an institution has a significant security breach or incident. As described in the *Federal Financial Institutions Examination Council (FFIEC) Information*

[1] *Security event is defined as an event that potentially compromises the confidentiality, integrity, availability, or accountability of an information system.*

[2] *Federal Financial Institution Examination Council (FFIEC) Information Security IT Handbook.*

[3] *A security breach or incident is defined by FFIEC as a security event that results in unauthorized access to data, applications, services, networks, or devices by bypassing underlying security mechanisms.*

Technology Examination Handbook (IT Handbook) on Information Security, management should define thresholds for reporting security incidents internally, and develop processes for when the institution should notify its regulator of incidents that may affect the institution's operations, reputation, or sensitive customer information. At a minimum, FCA expects System institutions to notify FCA for the following security and business continuity events:

- An incident or breach[4] using computer networks that results in an adverse effect on an information system or the information residing therein. For example, malware that has entered the institution's network resulting in server(s) being quarantined and memory/storage devices replaced and reimaged from a previously known malware-free state;
- Any loss of customer personally identifiable information (PII), or sensitive personal information (SPI). If devices such as laptops, smart phones, or tablets with PII or SPI are appropriately encrypted and managed, then management does not need to report lost or stolen devices to FCA. However, board reporting should be required;
- Any wire fraud attempts in which the perpetrator(s), whether successful or not, initiated a wire through an email account takeover or any other means. In accordance with FCA Regulation 609.930(i), System institutions should promptly report any known or suspected criminal violations associated with E-commerce to law enforcement authorities and FCA under part 612, subpart B - Referral of Known or Suspected Criminal Violations; and,
- Any event that requires the institution to activate its business continuity plan.

Given the increasing threat of cyber-attacks involving destructive malware and the impact these attacks can have on an institution's operation, reputation, and safety and soundness, FCA expects System institutions to maintain robust cyber resiliency.[5] This should include incident response and business continuity planning processes to mitigate the impact of these attacks on operations. Consistent with guidance from other regulatory agencies, FCA believes that all System institutions should take appropriate risk mitigation steps, including the following:

- Securely configure and maintain systems and services;
- Review, update, and test incident response and business continuity plans;
- Conduct ongoing information security risk assessments;
- Perform security monitoring, prevention, and risk mitigation;
- Protect against unauthorized access;
- Implement and test controls around critical systems regularly;
- Enhance information security awareness and training programs; and,
- Participate in industry information-sharing forums.

[4] *An attack, via cyberspace, targeting an institution for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; destroying the integrity of the data; or stealing controlled information.*

[5] *Cyber resilience is the ability of a system or domain to withstand cyber-attacks or failures and, in such events, to reestablish itself quickly.*

Training should support security awareness and strengthen compliance with security and acceptable use policies. Security should start with the board and management setting the appropriate tone at the top. Training programs should include scenarios capturing areas of significant and growing concern, such as phishing and social engineering attempts, loss of data through email or removable media, or unintentional posting of confidential or proprietary information on social media. As the risk environment changes, so should the training. Management should collect signed acknowledgments of the employee acceptable use policy as part of the training program, annually. In addition, periodic audits should be completed to test compliance with the institution's security policies and their overall effectiveness.

If a security incident or business continuity activation occurs, the institution's board or management should promptly notify FCA and provide a timely follow-up report on your institution's response and recovery actions. Incident response and business continuity plans should include directions to notify FCA's Office of the Chief Examiner at 1-888-244-3365.[6]

If you have any questions about this Informational Memorandum, please contact Operations Risk Program Manager Michael A. Anderson at (720) 213-0909 or by email at andersonm@fca.gov.

[6] *The Federal Agricultural Mortgage Corporation should notify FCA's Office of Secondary Market Oversight at 703-883-4280.*