Federal Housing Finance Agency
Office of Inspector General

Cyber Security: An Overview of FHFA's Oversight of and Attention to the Enterprises' Management of Their IT Infrastructures

White Paper • WPR-2015-003 • March 31, 2015

EXPLANATION OF REDACTIONS IN THIS REPORT

This report includes redactions intended to protect from disclosure material that FHFA asserts is confidential financial, proprietary business, and/or trade secret information. The redacted information would not ordinarily be publicly disclosed, and, if disclosed, could disadvantage Freddie Mac and Fannie Mae.

WPR-2015-003

March 31, 2015

Executive Summary

Over the past 10 years, individuals, institutions, and the U.S. economy and infrastructure have become heavily dependent on digital highways. Until recently, the common public perception was that the systems controlling these highways were secure and that data on these systems was protected. However, cyber breaches over the past year have focused public attention on the insecurity of these systems and demonstrate how vulnerable the private sector has become. Some of these breaches have been merely annoying – like the offensive posts on Crayola's Facebook page or in Chipotle's Twitter feed, while others involved wholesale theft of corporate and personal data – like the assaults on Anthem Inc., Sony Pictures, JPMorgan, Home Depot, and Target that caused significant reputational and economic damage. According to a survey by PwC of 9,700 respondents world-wide, the compound annual growth rate of detected cyber attacks increased 66% year-over-year since 2009 and entities with gross annual revenue in excess of $1 billion reported 44% more cyber attacks than for the prior year. Even though JPMorgan spent $250 million in 2014 on its cyber security, the controls it put into place did not prevent the massive hack.

Cyber attacks pose a diverse and often dangerous threat for institutions worldwide. Cyber criminals appear particularly keen on stealing customer information (like names, addresses, phone numbers, account numbers, passwords, user IDs, dates of birth, or Social Security numbers), trade secrets, or other confidential information and compromising the credentials of a legitimate user to commit financial fraud. Moreover, hackers may also have motivations other than theft; for example, cyber attackers skilled in information technology as well as with the controls systems and production processes of an iron plant in Germany exploited vulnerabilities in the computer system to cause a blast furnace to explode and destroy the plant. NSA Director Rogers has reported that, over the past few years, cyber threat actors are becoming more adept at gaining the technology needed to launch crimes against critical U.S. infrastructures in an effort to selectively shut down parts of the power grid and other utilities. Additionally, a November 2014 report from the international standard-setting Committee on Payments and Market Infrastructures warned that stock exchanges, settlement systems, and clearing houses around the world have become increasingly vulnerable to cyber attacks, and a sophisticated cyber attack could interrupt or destabilize financial markets.

Fannie Mae and Freddie Mac (collectively, the Enterprises) are the two largest institutions issuing mortgage-related securities in the U.S. secondary mortgage market. They store, process, and transmit financial data and personally identifiable information in connection with their mission to support the

WPR-2015-003

March 31, 2015

secondary mortgage market. As events over the past year have shown, other organizations holding similar types of data have sustained significant cyber attacks. The Enterprises recognize, in recent annual securities filings, that there is no assurance that their substantial precautions to protect data will be invulnerable to penetration and that a successful cyber attack could lead to substantial financial losses.

In this white paper, OIG summarizes the types of known cyber threats in the current environment and discusses the possible risks to the Enterprises from such threats. We also provide an overview of the Enterprises' cyber risk management practices to prevent and detect cyber attacks as well as the oversight of such practices by the Enterprises' regulator and conservator, the Federal Housing Finance Agency (FHFA).

OIG recognizes the significant financial, governance, and reputational risks that could flow from a cyber attack on the Enterprises. OIG plans to assess the adequacy of FHFA's oversight of the Enterprises' information technology security and study the Enterprises' controls for information technology security to evaluate whether FHFA and the entities under its conservatorship have sufficiently addressed possible vulnerabilities in information technology security.

This white paper was produced by an interdisciplinary team from OIG's Office of Investigations and Office of Audits. The team included Paul Conlon, Assistant Inspector General for Investigations; Stephan Reimers, Senior Special Agent; Joi Neal, Senior Auditor; Michael Kim, Auditor; Daniel Rose, IT Specialist – Audits; Mark Hengst, Special Agent; and Charlie Divine, Investigative Counsel.

We appreciate the assistance of the officials from FHFA and the Enterprises in completing this white paper.

This white paper has been distributed to Congress, the Office of Management and Budget, and others and will be posted on FHFA-OIG's website: www.fhfaoig.gov.

Rene Febles
Deputy Inspector General for Investigations

TABLE OF CONTENTS

ABBREVIATIONS

AB	Advisory Bulletin
CISO	Chief Information Security Officer
Enterprises	Fannie Mae and Freddie Mac
Fannie Mae	Federal National Mortgage Association
FFIEC	Federal Financial Institutions Examination Council
FHFA	Federal Housing Finance Agency
FHLBanks	Federal Home Loan Banks
Freddie Mac	Federal Home Loan Mortgage Corporation
FS-ISAC	Financial Services Information Sharing and Analysis Center
HERA	Housing and Economic Recovery Act of 2008
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IT	Information Technology
MBS	Mortgage-Backed Securities
NIST	National Institute of Standards and Technology
OIG	Federal Housing Finance Agency, Office of Inspector General
PII	Personally Identifiable Information

BACKGROUND

Cyber Attackers Are on the Rise Using Different Tools and Techniques

In 2012, then-FBI Director Robert Mueller warned that cyber attacks on American companies were "no longer a question of 'if' but 'when' and 'how often.'" He was "convinced that there are only two types of U.S. companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again."[1] Information security experts have opined that 2014 "will long be remembered for a series of mega security breaches and attacks" and predict that 2015 will be "as bad or worse."[2]

Organizations have long been vulnerable to physical thefts of tangible property or misuse of assets by a determined insider. Now, those vulnerabilities have enlarged to include the organization's assets in electronic form. Employees and contractors, current or former, with authorized access to an organization's network or data can exceed or misuse access and compromise the confidentiality, integrity, or availability of the organization's information or information systems. Even when an organization builds high barriers to protect its electronic assets from outsiders, many have few protections against insiders. In September 2014, the FBI and Department of Homeland Security warned employers about the rise in insider hacking, cautioning that cloud storage or software that permits remote access to corporate networks had been used by insiders to access and steal trade secrets and other confidential materials.[3]

According to the PwC 2014 U.S. State of Cybercrime Survey of U.S. businesses, law enforcement, and government agencies, a third of the respondents replied that insider cyber attacks were more costly or damaging than attacks by outsiders. Insiders typically have greater access to sensitive information, a better understanding of internal processes, and an understanding of potential weaknesses in controls. Depending upon the degree of legitimate access provided to an insider and the length of time in which that insider can act, a cyber attack by an insider can be devastating, as Edward Snowden has shown. Mr. Snowden, who worked as a technology consultant to the NSA in Hawaii, was tasked with managing NSA's computer systems in an office focused on China and North Korea and his permissions

---

[1] Federal Bureau of Investigation, *Remarks of FBI Director Robert S. Mueller, III to RSA Cyber Security Conference in San Francisco, CA* (Mar. 1, 2012) (online at www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies).

[2] Ponemon Institute, *2014: A Year of Mega Breaches*, at 1 (Jan. 22, 2015).

[3] *See* Internet Crime Complaint Center, *Public Service Announcement: Increase in Insider Threat Cases Highlight Significant Risks to Business Networks and Proprietary Information* (Sept. 23, 2014) (online at www.ic3.gov/media/2014/140923.aspx).

provided broad access to NSA files. U.S. intelligence officials determined that Mr. Snowden used a web crawler, an "inexpensive and widely available software, to 'scrape' the National Security Agency's networks" automatically, using parameters he had set, "while he went about his day job."[4] These investigators found that Mr. Snowden's insider attack was hardly sophisticated.

Cyber attacks emanating from outside an organization come in numerous forms. Among the most widely used attack vehicles are denial-of-service;[5] phishing scams;[6] social engineering;[7] viruses, worms, and password attacks;[8] and malware[9] to infiltrate secure systems. Broadly speaking, external cyber attackers can be grouped into three categories: "hacktivists," nation states, and criminals.

- ***Hacktivists.*** Individuals or groups who use digital tools to promote a political or social agenda are often labeled "hacktivists." Hacktivists see themselves as anonymous caped crusaders, using technology to bring about social or political change and/or as a tool for political speech. Others view them as cyber terrorists for their efforts to post offensive comments on Twitter or Facebook accounts of others, defacing websites for political reasons, attacking websites of groups and governments that oppose their ideology, and in taking control of websites to significantly compromise them.

- ***External Attacks: Nation-State Hacking.*** Over the past few years, reported attempts by foreign intelligence to obtain illegal or unauthorized access to confidential

---

[4] David Sanger and Eric Schmitt, *Snowden Used Low-Cost Tool to Best N.S.A.*, The New York Times (Feb. 8, 2014) (online at www nytimes.com/2014/02/09/us/snowden-used-low-cost-tool-to-best-nsa html?hp&_r=2).

[5] A denial of service attack is intended to compromise the availability of networks and systems by overloading the network, thereby limiting legitimate traffic or communication. This type of attack can be done in a distributed fashion from many sources at once.

[6] The FTC defines phishing as "When internet fraudsters impersonate a business to trick you into giving out your personal information[.]" Federal Trade Commission, *Consumer Information: Phishing* (online at www.consumer ftc.gov/articles/0003-phishing).

[7] Social engineering is used to secretly install spyware or other malicious software or to trick someone into handing over passwords or other sensitive information. Social engineering scams can include email messages that ask the recipient to open an attachment.

[8] Password attacks involve the use of software to crack a user's password so that the attacker may obtain access to a secured system. The software systematically checks all possible keys or passwords until the correct one is found.

[9] Malware, or malicious software, is computer code that includes viruses, worms, and Trojan horses aimed at gaining control of systems. Kaspersky Lab, a Moscow-based information security firm, reported that it saw a tenfold increase in mobile malware over the last year and evaluates 325,000 pieces of new malware each day. Brian Fung, *The Switch: The Time a Major Financial Institution was Hacked in under 15 Minutes*, The Washington Post (Jan. 14, 2015) (online at www.washingtonpost.com/blogs/the-switch/wp/2015/01/14/the-time-a-major-financial-institution-was-hacked-in-under-15-minutes/).

information in U.S. companies have continued to rise. The Defense Security Service (DSS), in annual reports analyzing all foreign efforts to gain improper access to electronic data stored by U.S. companies, has found that those efforts were directed toward obtaining technology, intellectual property, trade secrets, and proprietary information.[10] While DSS found that a portion of the hacking activity emanating from outside the U.S. was attributable to foreign commercial collectors, it also found that the share attributed to foreign government and government-affiliated entities in East Asia and the Near East significantly increased over the past few years.

- In May 2014, five Chinese men, officers in the Chinese People's Liberation Army, were indicted on charges of computer hacking and espionage arising from efforts to hack into six American companies in the U.S. nuclear power, metals, and solar products industries; this marked the first time that criminal charges were filed against state actors for hacking.[11] Shortly thereafter, a U.S. security research firm issued a report accusing a second Chinese military unit of carrying out cyber espionage against foreign corporations.[12]

- After the FBI determined that North Korea launched the destructive cyber attack on Sony Pictures, President Obama issued an executive order imposing additional sanctions on that country.[13]

- The U.S. government is not immune from foreign cyber espionage. The former head of the FBI's cyber division attributed Russian hacking into the email systems at the White House and State Department, and Chinese hacking into National Weather Service computers and the personal data of 800,000 employees from the U.S. Postal Service to "most likely an intelligence collection operation. They are looking to gather intelligence about who the

---

[10] *See, e.g.*, DSS, *Targeting U.S. Technologies: A Trend Analysis of Cleared Industry Reporting* (2013) (online at www.dss mil/documents/ci/2013%20Unclass%20Targeting%20US%20Technologies_FINAL.pdf); DSS, *Targeting U.S. Technologies: A Trend Analysis of Cleared Industry Reporting* (2014) (online at www.dss mil/documents/ci/2014UnclassTrends.PDF).

[11] FBI, *Five Chinese Military Hackers Charged with Cyber Espionage Against U.S.* (May 19, 2014) (online at www fbi.gov/news/news_blog/five-chinese-military-hackers-charged-with-cyber-espionage-against-u.s).

[12] Charles Riley, *Second Chinese Military Unit Linked to Hacking*, CNN Money (June 10, 2014) (online at http://money.cnn.com/2014/06/10/technology/china-military-cyberattacks/index html).

[13] Devin Dwyer, *President Obama Sanctions North Korea after Sony Cyberattack*, ABC News (Jan. 2, 2015) (online at http://abcnews.go.com/Politics/obama-sanctions-north-korea-sony-cyberattack/story?id=27965524).

players are within the government, who they are communicating with, etc., and the new initiatives they are developing."[14]

- Most recently, investigators looking into the data breach at Anthem Inc. reviewed evidence that suggests that Chinese state-sponsored hackers were responsible for the theft.[15]

- These types of attacks led FBI Director Comey to warn, "There are two kinds of big companies in the United States…those who've been hacked by the Chinese and those who don't know they've been hacked by the Chinese."[16]

- ***External Attacks: Criminals in Cyberspace.*** Criminal activity conducted over the Internet is called cyber crime. Cyber attacks can include stealing an organization's intellectual property or confidential information, taking illegal financial control of the accounts of others, and/or disrupting infrastructure operations of a company or country. As shown by the recent annual report of the Ponemon Institute, cyber crime continues to rise for organizations in all industries.[17] That report also found that information theft remains the most expensive consequence of a cyber crime, followed by business disruptions, loss of revenue, and damage to equipment.

  - *Direct cyber attack on an organization's systems.* Cyber criminals have demonstrated an appetite for confidential financial market information. In 2011, the International Monetary Fund suffered a major cyber attack and concluded that the intention was not to steal personal information for fraud purposes, but to gain sensitive "insider privileged information."[18] Organizations that engage in market activities that provide access to a substantial amount of non-public financial information are attractive targets

---

[14] Bob Orr, *Spate of Cyber Attacks Target U.S. Government Systems*, CBS News (Nov. 17, 2014) (online at www.cbsnews.com/news/spate-of-cyber-attacks-target-us-government-systems/).

[15] David Stout, *Chinese Hackers May Be Responsible for the Anthem Attack, Reports Say*, Time Inc. (Feb. 5, 2015) (online at http://time.com/3698417/china-anthem-hack-healthcare/).

[16] 60 Minutes, *Interview with FBI Director James Comey*, CBS (Oct. 5, 2014) (online at www.cbsnews.com/news/fbi-director-james-comey-on-threat-of-isis-cybercrime/). Following that warning, the FBI cautioned U.S. businesses that "Chinese Government affiliated cyber actors" were engaged in stealing "high-value information from U.S. commercial…networks through cyber espionage." Reuters, *FBI Warns U.S. Businesses of Cyber Attacks, Blames Beijing* (Oct. 15, 2014) (online at www reuters.com/article/2014/10/15/us-usa-cybersecurity-china-idUSKCN0I42MU20141015).

[17] Ponemon Institute, *2014 Global Report on the Cost of Cyber Crime* (Oct. 30, 2014).

[18] *See* Jim Wolf and William MacLean, *IMF Cyber Attack Aimed to Steal Insider Information: Expert*, Reuters (June 12, 2011) (online at www.reuters.com/article/2011/06/12/us-imf-cyberattack-idUSTRE75A20720110612) (accessed Dec. 2, 2014).

for a cyber attack. During the recent attack on Sony Pictures Entertainment, the FBI stated the attack resulted in the "theft of proprietary information as well as employees' personally identifiable information and confidential communications."[19] Cyber attacks on Home Depot and Target, for example, underscore the acute interest in theft of personally identifiable information (PII) and associated identify theft and credit card fraud.[20]

- *Indirect cyber attack through third parties.* As internal control environments within organizations are strengthened, cyber criminals have begun to target trusted third-party vendors (like law firms), contractors, counterparties, partners, and/or affiliates as the origin of attack because they generally have fewer security controls in place and are considered softer and easier to exploit. Where a third party has regular access to data behind an organization's firewalls, cyber criminals who infiltrate a third-party's systems may be able to access the organization's data by masquerading as the third party.[21] With more organizations using public cloud services for data storage and those organizations dependent on the security provided by cloud providers, cloud computing has become a target as well.

Cyber Risks for the Enterprises

Commercial cyber criminals typically look at the attractiveness of the data held by potential targets, monies that can be easily stolen, and the ease of breaching the target. In October 2014, the U.S. Senate Committee on Banking, Housing, and Urban Affairs sought information on cyber security protections in place at the Department of the Treasury, the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, and the Office of the Comptroller of the Currency. That request cited the views of the then Director of the National Cybersecurity and Communications Integration Center at the Department of Homeland Security; he opined that, of the 16 critical

---

[19] *See* FBI, *Update on Sony Investigation* (Dec. 19, 2014) (online at www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation).

[20] *See* Social Security Administration, *Identity Theft And Your Social Security Number*, at 2 (Dec. 2013) (online at www.ssa.gov/pubs/10064 html) (accessed Dec. 2, 2014).

[21] Because "a firm's level of cybersecurity is only as good as the cybersecurity of its vendors," the New York State Department of Financial Services recently sought information from large New York banks relating to third-party vendors' information security risks, including the protections used to safeguard sensitive data when communicating with third-party vendors. Emily Glazer, *Lawsky Targets Banks' Cyberattack Vulnerability*, The Wall Street Journal (Oct. 21, 2014) (online at www.wsj.com/articles/lawsky-targets-banks-cyberattack-vulnerability-1413941506).

infrastructure sectors in this country, "finance probably wins the cyber security threat award…[The industry is] a massive target…because [it is] where the money is."[22]

The Enterprises are the two largest sources of residential mortgage-backed securities in the U.S. secondary mortgage market. As of September 2014, Fannie Mae guaranteed 17.6 million single-family mortgage loans and Freddie Mac guaranteed 10.6 million. Together, the Enterprises held or guaranteed approximately $5 trillion in mortgage assets supporting the U.S. mortgage market as of November 2014.

As part of their processes to guarantee or purchase loans, the Enterprises receive significant information about a borrower, including financial data and PII. [redacted]. The quantity and quality of PII possessed by the Enterprises is likely to increase over time as they comply with an FHFA directive to standardize mortgage data fields and collect loan data at a more granular level. The PII and confidential financial data obtained by the Enterprises is regularly shared with third parties, such as foreclosure specialists and mortgage servicers. [redacted]

Based on recent cyber attacks on other entities holding similar types of information, a cyber attack on one of the Enterprises could occur directly or indirectly, such as on lenders from which the Enterprises purchase mortgages, mortgage servicers, contract realtors, outside law firms, collection agents, foreclosure and bankruptcy services consultants, and ratings agencies, and could involve the theft of PII and/or material non-public information.

If the Enterprises were to suffer a significant cyber attack, the tangible costs of responding could include rebuilding compromised computer systems, purchasing credit monitoring for customers, and designing and implementing additional controls.

[22] Securities and Exchange Commission, *Cybersecurity Roundtable*, Statement of Larry Zelvin (Mar. 26, 2014) (online at www.sec.gov/news/otherwebcasts/2014/cybersecurity-roundtable-032614.shtml).

[redacted]

CYBER ATTACKS AT THE ENTERPRISES .....

The Enterprises have been the subject of cyber attacks from internal and external actors in the recent past, although none of these attacks caused harm of any significance. OIG has investigated a number of these attacks and its investigations found motives ranging from politically driven hacktivism to PII theft.

In their 2012 and 2013 Form 10-K Annual Reports filed with the SEC, both Enterprises identified cyber attacks and other unauthorized access, disclosure, and disruption as a material risk to their business operations.[24]

CYBER SECURITY CONTROLS AT THE ENTERPRISES.....

Responsibility for Cyber Security

As conservator of the Enterprises, FHFA is vested with express authority to operate each entity. As discussed in our recent white paper,[25] FHFA has determined to (1) delegate authority for general corporate governance and day-to-day matters to the Enterprises' boards of directors and executive management and (2) retain authority for certain significant decisions.[26] Management of cyber security is not an area expressly retained by FHFA. Absent a decision by the FHFA Director to intervene in a cyber security matter, the Enterprises bear responsibility for cyber security and FHFA oversees the adequacy of the Enterprises' cyber security programs and controls as their regulator.

The Enterprises recognize the need to continually enhance their cyber security controls and have endeavored to create a structural framework to protect their cyber systems. Not unlike many U.S. companies, the Enterprises have been subject to cyber attacks and have taken remedial measures to prevent another such attack.

---

[24] *See* Fannie Mae, *2012 Form 10-K* (online at www.sec.gov/Archives/edgar/data/310522/000031052213000065/fanniemae201210k.htm) (accessed Jan. 13, 2015); Freddie Mac, *2012 Form 10-K* (online at www.freddiemac.com/investors/er/pdf/10k_022813.pdf) (accessed Jan. 13, 2015); Fannie Mae, *2013 Form 10-K* (online at www fanniemae.com/resources/file/ir/pdf/quarterly-annual-results/2013/10k_2013.pdf) (accessed Nov. 17, 2014); and Freddie Mac, *2013 Form 10-K* (online at www.freddiemac.com/investors/er/pdf/10k_022714.pdf) (accessed Nov. 17, 2014).

[25] FHFA-OIG, *FHFA's Conservatorships of Fannie Mae and Freddie Mac: A Long and Complicated Journey* (Mar. 25, 2015).

[26] For general background on FHFA's delegations of authority to the Enterprises, *see* FHFA-OIG, *FHFA's Conservator Approval Process for Fannie Mae and Freddie Mac Business Decisions* (Sept. 27, 2012) (AUD-2012-008) (online at www.fhfaoig.gov/Content/Files/AUD-2012-008_2.pdf).

Each Enterprise has specific internal cyber security policies and procedures and conducts regular vulnerability assessments. Fannie Mae tests its employees and contractors every month on their understanding of cyber security practices, and employees who lack sufficient knowledge of these practices are subject to supplementary information security training. Each Enterprise monitors state and federal regulations related to cyber security and privacy protection.

With respect to the third parties and counterparties with whom they do business, the Enterprises report that third-party vendors and counterparties are obligated by contract to maintain appropriate controls. Each conducts security assessments on a regular basis on third-party vendors that it deems critical and requires contractors to satisfy specific security training requirements.[27]

To stay current about cyber threats, the Enterprises participate in the Financial Services Information Sharing and Analysis Center (FS-ISAC), which is the global financial industry's central resource for cyber and physical threat intelligence analysis and sharing. Recently, they have begun to share threat intelligence on an ad-hoc basis, prompted by a 2014 spear phishing[28] cyber attack on one of them. OIG was advised by each Enterprise that FHFA has not issued a formal directive regarding sharing of threat intelligence. A senior FHFA official reported to OIG that FHFA has not insisted upon sharing threat information because each Enterprise has dedicated significant resources to gathering its own intelligence.

FHFA requires each Enterprise to report significant cyber incidents, [redacted] Each Enterprise makes its own determination on whether to report cyber incidents and impact to FHFA. According to Fannie Mae, it reports to FHFA all cyber incidents that would likely cause heightened reputational risk to it, including any data breaches, on a weekly basis. Freddie Mac reported that security incidents are discussed with the FHFA exam team during scheduled monthly discussions.

The Enterprises are required to notify consumers of data breaches involving PII. Both Enterprises have established similar procedures and controls for reporting these cyber incidents.

[27] Details regarding the Enterprises internal controls were obtained from Enterprise documents and interviews of Enterprise and FHFA employees. OIG did not test the Enterprises' internal cyber security controls or their assessment of third parties in preparing this white paper.

[28] Spear phishing is a subcategory of phishing attacks. Spear phishing attacks use personal information such as name or job title to lull unsuspecting victims into assuming an email or attachment is meant for them and therefore harmless.

Acting as regulator, FHFA issued an advisory bulletin in May 2014 to provide guidance for a risk-based approach to cyber security management[29] and incorporated assessment of the adequacy of cyber security controls into its examination program.

FHFA supervises the Enterprises by creating and executing annual examination plans reflecting the Agency's supervision strategy. The annual plans can incorporate targeted reviews and ongoing monitoring. The FHFA examination manual, which describes FHFA's standards and expectations for its examinations, aids FHFA examiners in conducting exams. One section of that manual, the Information Technology Risk Management Program (effective August 2013, Version 1.0), provides guidance on how to evaluate and assess the Enterprises' IT operations, including topics related to cyber security management [redacted]

In addition to these examinations, FHFA gathers information about the adequacy of the Enterprises' cyber security controls from other sources, including operational risk reports and required reports from the Enterprises, the ad-hoc exchange of information with Enterprise management, and external sources.

CONCLUSION

Recent cyber attacks against Sony, Target, JPMorgan, and Anthem, among others, make clear that organizations holding PII and financial data are vulnerable to such attacks. While past cyber attacks on the Enterprises have not caused harm of any significance, both Enterprises acknowledge the increasing number and sophistication of cyber attacks and recognize that the substantial precautions put into place to protect data may not be invulnerable to penetration. In this regard, the cyber threat to the Enterprises is no different than such threat to any other major financial institution.

OIG recognizes the significant financial, governance, and reputational risks that could flow from a cyber attack on the Enterprises. Over the coming year, OIG plans to assess the

[29] FHFA, *Advisory Bulletin: Cyber Risk Management Guidance* (May 19, 2014) (AB-2014-05) (online at www fhfa.gov/SupervisionRegulation/AdvisoryBulletins/Pages/AB-2014-05-Cyber-Risk-Management-Guidance.aspx). *See also* Appendix B in this report.

[redacted].

adequacy of FHFA's oversight of the Enterprises' information technology security and study the Enterprises' controls for information technology security to assess whether FHFA and the entities under its conservatorship have sufficiently addressed possible vulnerabilities in information technology security.

OBJECTIVE, SCOPE, AND METHODOLOGY .....

The objectives of this white paper report were to provide a perspective into FHFA's oversight of the Enterprises' cyber security programs, to discuss cyber attacks at the Enterprises, and to discuss cyber risk management practices employed by the Enterprises.

To address this report's objectives, we interviewed the Enterprises' Chief Information Officers and CISOs as well as officials responsible for information security management. We also interviewed officials from FHFA's Division of Conservatorship Operations and Division of Enterprise Regulation, as well as FHFA's CISO.

In addition, we reviewed a variety of public resources as well as non-public information provided by the Enterprises and FHFA. The data used in this report covered the period 2012 through the third quarter of 2014, when available.

The performance period for this white paper report was from November to December 2014.

We appreciate the efforts of FHFA, the Enterprises, and their staff in providing information and access to necessary documents to accomplish this study.

APPENDIX A .....

Types of Cyber Attacks and Attackers

FIGURE 1. TYPES OF CYBER ATTACKS

Attack Type	Description
WEB APPLICATION ATTACKS	Any attack in which a web application is the vector of attack. This includes exploits of code level vulnerabilities in the application, as well as bypassing authentication mechanisms.
INSIDER AND PRIVILEGE MISUSE	Any unapproved or malicious use of organizational resources. Mostly insiders are the culprits of the misuse, but colluding outsiders and partners can also be sources of attack because of privileges granted to them due to relationships and trusts.
DENIAL OF SERVICE ATTACKS	Any attack intended to compromise the availability of networks and systems by overloading the network, thereby limiting legitimate traffic or communication. This type of attack can be done in a distributed fashion from many sources at once.
MALWARE ATTACKS	Malicious computer code that includes viruses, worms, and Trojan horses aimed at gaining control of systems.[31] Malware exploits existing or unknown vulnerabilities on systems and software applications to introduce computer code that will provide persistent access to the system and exfiltrate user data. Malware can be introduced by duping unsuspecting users through social engineering exploits, such as email phishing.
POINT-OF-SALE INTRUSIONS	Remote attacks against environments where retail transactions are conducted and where card purchases are made. These attacks involve tampering with access devices.
PHYSICAL THEFT AND LOSS	Any incident where an information asset containing financial, competitive, personal, customer, or intellectual property went missing through loss or theft.
CYBER ESPIONAGE	Unauthorized network or system access linked to state-affiliated actors or multinational corporations for the purpose of stealing trade secrets and confidential data.

FIGURE 2. TYPES OF CYBER ATTACKERS[32]

Attacker Type	Motivation
CYBER CRIMINAL	Cyber criminals are professionals who use malware and exploits to steal money. Their motivation is quick, large financial gain.
SPAMMERS AND ADWARE SPREADERS	Developers of spam and adware make their money through illegal advertising, either getting paid by a legitimate company for pushing business their way or by selling their own products.

[31] Symantec, *Malware* (online at http://us.norton.com/security_response/malware.jsp).

[32] *See* Roger Grimes, *Your Guide to the Seven Types of Malicious Hackers*, InfoWorld (Feb. 8, 2011) (online at www.infoworld.com/article/2623407/hacking/your-guide-to-the-seven-types-of-malicious-hackers.html).

Attacker Type	Motivation
ADVANCED PERSISTENT THREAT (APT) AGENTS	Intruders engaging in APT-style attacks represent well-organized, well-funded groups, often located in a "safe harbor" country. APT agent attacks require a high degree of covertness over a long period of time and are geared toward accessing sensitive and/or intellectual property information. The motivation for such attacks is consistent with cyber warfare and/or corporate espionage.
CORPORATE SPIES	Corporate spies are interested in obtaining intellectual property or competitive information for sale. Corporate espionage groups are not usually as organized as APT groups, and they are more focused on short- to mid-term financial gains made off of the sale of corporate secrets.
HACKTIVISTS	Hacktivists are hackers who are motivated by political, religious, environmental, or other personal beliefs. They are usually content with embarrassing their opponents or defacing their websites.
CYBER WARRIORS	Cyber warfare is a state-sponsored exploitation with an endgame objective of disabling an opponent's military capability. Participants may operate as APT or corporate spies at times, but everything they learn is geared toward a specific military objective.
ROGUE HACKERS	Rogue hackers simply want to prove their skills, brag to friends, and are thrilled to engage in unauthorized activities.

APPENDIX B.....

Seven Factors To Be Considered, as Directed by *Cyber Risk Management Guidance, AB-2014-05*

This Advisory Bulletin provides considerations and expectations for a risk-based approach to cyber security management and identifies seven factors the regulated entities should consider.

1. Proportionality: The regulated entities' cyber risk management programs should be proportional to the unique cyber risks of the Enterprises and regulated entities.

2. Cyber Risk Management: The regulated entities should leverage existing risk management practices.

3. Risk Assessments: The regulated entities should conduct regular risk assessments to identify, understand, and prioritize cyber risks.

4. Monitoring and Response: The regulated entities should identify cyber risks through the application of a cyber risk management program.

5. System, Patch, and Vulnerability Management: The regulated entities should facilitate the regular assessment and timely repair of vulnerabilities in systems and applications.

6. Third Party Management: The regulated entities should recognize, monitor, and prioritize the mitigation of the substantial risks posed by third-party access to the regulated entities' data and systems.

7. Privacy and Data Protection: The regulated entities should protect sensitive and confidential data and PII in their possession to reasonably safeguard against legal and reputational risk.

ADDITIONAL INFORMATION AND COPIES.....

For additional copies of this report:

- Call: 202-730-0880
- Fax: 202-318-0239
- Visit: www.fhfaoig.gov

To report potential fraud, waste, abuse, mismanagement, or any other kind of criminal or noncriminal misconduct relative to FHFA's programs or operations:

- Call: 1-800-793-7724
- Fax: 202-318-0358
- Visit: www.fhfaoig.gov/ReportFraud
- Write:

  FHFA Office of Inspector General
  Attn: Office of Investigation – Hotline
  400 Seventh Street, S.W.
  Washington, DC 20024