U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE
CHAIRMAN FRED UPTON

The Oversight Series

Accountability to the American People

Information Security at the Department of Health and Human Services

Prepared by the Energy and Commerce Committee, Majority Staff

Executive Summary

On October 15, 2013, the Food and Drug Administration (FDA) suffered a breach of its internal network. An unauthorized user gained access to the account details of over 14,000 users of one of FDA's information systems. While the breach did not result in substantial harm to the agency's network and users, it highlighted the susceptibility of FDA's network to attacks and raised questions about the adequacy of FDA's information security program. To examine these questions, the Energy and Commerce Committee began an investigation into FDA's information security in December 2013.

During the investigation, committee staff became aware of several other information security incidents at FDA and other Department of Health and Human Services (HHS) operating divisions. To the committee's knowledge, five HHS operating divisions have been breached using unsophisticated means within the last three years. Of concern to the committee, officials at the affected agencies often struggled to provide accurate, clear, and sufficient information on the security incidents during the committee's investigation.

Further, the committee became aware of non-public HHS Office of Inspector General (OIG) reports on HHS information security over the last seven years, which reveal pervasive and persistent deficiencies across HHS and its operating divisions' information security programs. The OIG reports, in combination with the operating divisions breaches and the inability of agency officials to provide accurate and sufficient information about them, suggest weaknesses exist within the information security practices of both HHS and its operating divisions.

Many of the information security issues suffered by HHS operating divisions shared the same root cause. At FDA, the Centers for Medicare and Medicaid Services (CMS), and the Office of Civil Rights (OCR), security concerns were subordinated to operational concerns. Evidence from the committee's investigation indicates that this stems from the organizational relationship and division of authorities between the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) at both HHS headquarters and throughout its operating divisions, which prioritizes operational over security concerns, resulting in security interests receiving insufficient or improper attention.

Prioritizing operations over information security concerns also degrades the overall adequacy of information security programs at HHS and its operating divisions. The committee's investigation revealed several issues that raised questions as to whether information security personnel have the appropriate authorities, and in some cases, the expertise necessary to carry out their duties. For example, the investigation found:

(1) Audits of information security at two operating divisions were constrained due to operational concerns and incompleteness. In both cases, the CIO-CISO hierarchy prevented the CISO from requiring full system audits.

(2) Information security officials are not always permitted full visibility into their own networks as a result of their relationship with agency contractors, who may own and operate portions of agency networks.

(3) Two information security breaches at two different operating divisions resulted from misconfigurations. A separate breach resulted from a missing "critical" software patch. These incidents raise questions about whether information security officials have the appropriate level of expertise.

(4) The information security officials at one operating division misidentified a list of hacker aliases as a list of security vulnerabilities.

(5) Officials at two operating divisions were unable to provide accurate information about security incidents within their own networks.

Under the Federal Information Security Management Act (FISMA), federal agencies are required to hire a CIO to manage information technologies, and also a CISO to manage information security. FISMA further requires that CISOs report to CIOs. HHS complies with these requirements.

After examining the October 15, 2013 breach of FDA's network, and other breaches of HHS information systems, it is clear that the relationship between the CIO and the CISO in HHS's headquarters and its operating divisions is an important factor contributing to the prioritization of operational concerns over security concerns. These issues could be resolved by moving the CISO position to the Office of the General or Chief Counsel, as applicable. The separation of the management of information technology from the management of information security concerns would remove information security from the information technology "silo" and would facilitate the inclusion of expertise across HHS in information security decisions. In particular, the placement of the CISO within the Office of the General or Chief Counsel specifically acknowledges that information security has evolved into a risk-management activity, traditionally the purview of the legal team. This reorganization is an important first step toward creating a system that incentivizes better security.

PART I – FDA INVESTIGATION AND RELATED INCIDENTS AT HRSA AND NIH

A. Information Security is Especially Important at the Food and Drug Administration

Attacks on federal information systems, including the systems of FDA, are on the rise. As noted by HHS' Office of Inspector General (OIG) and FDA's CIO, malicious actors are increasingly compromising government systems, publishing sensitive data, and using stolen data to commit fraud.[1,2] Furthermore, the nature of threats to federal agency web applications are continually changing due to new or advancing techniques leveraged by malicious actors, the release of new technology, and the deployment of increasingly complex systems.[3] Information technologies and web services that are not properly secured are vulnerable to unauthorized manipulation that may compromise the confidentiality of sensitive information or negatively affect the operations of federal agencies.[4] In an October 2014 report, OIG wrote:

> Today's cyber assaults are not the same as those seen in the past and often involve highly sensitive information shared by investigative partners involving a planned effort, put in place over a period of time, by an intelligent, patient, and skilled criminal element. Criminals utilize the best technology and seek out vulnerabilities, and often many are not yet known to system and software developers.[5]

FDA is the country's principal consumer protection and health agency, regulating about twenty-five percent of the gross domestic product, including the food supply, medical devices, drugs, vaccines, cosmetics, animal feed and drugs, and radiation-emitting items. In carrying out these responsibilities, the agency relies heavily on information technology (IT) to hold an enormous amount of important and sensitive information.[6] Such systems are critical to the agency's product review, adverse event reporting, and compliance activities.

FDA has the legal obligation to protect companies' trade secrets and confidential commercial information. To fulfill this responsibility, FDA must have an adequate data security program to meet these obligations. However, the vulnerability of information collected and maintained by FDA has been a concern for a number of years. In March 2012, the nonpartisan Government Accountability Office (GAO) issued a report, "Information Technology: FDA Needs to Fully

---

[1] DEPT. OF HEALTH AND HUMAN SERVICES, OFF. OF INSP. GEN., PENETRATION TEST OF THE FOOD AND DRUG ADMINISTRATION'S COMPUTER NETWORK (A-18-13-30331) (Oct. 2014), *available at* http://oig.hhs.gov/oas/reports/other/181330331.pdf.

[2] Statement of Walter S. Harris, Deputy Commissioner for Operations and Chief Operating Officer, FDA before the House Committee on Oversight and Government Reform, "Monitoring FDA Personnel's use of Agency Information Technology Systems," February 26, 2014.

[3] *Id.*

[4] *Id.*

[5] *See supra* note 1.

[6] FDA's websites experience more than 350 million hits, 25 terabytes of data transferred, and 6 million visitors per month. The FDA public web site supports FDA's mission in communicating to healthcare professionals and the public as effectively as possible. (FDA's Website Support and Hosting Services (WSHS) contract – HHSF223201000054I, Attachment 1 SOW, at 1 (2010)).

Implement Key Management Practices to Lessen Modernization Risks." The GAO found that although FDA reportedly spent about $400 million for IT investments in FY 2011,[7] the agency still lacked a comprehensive IT inventory that identified and provided key information about the systems it uses and those in development. The report also detailed a stalled effort to modernize FDA's systems estimated to cost $280 million, stating, "much of the planned functionality has not been delivered and its completion is uncertain." The government watchdog went on to conclude, "it is uncertain when or if FDA will meet its goals of replacing key legacy systems and providing modernized functionality to support its mission."

As part of its effort to protect its information systems, FDA does follow FISMA requirements. FISMA requires that government agencies hire a CIO to manage their information technologies to ensure networks and sensitive data are adequately managed and protected. It also requires that agencies hire a CISO, to whom the CIO designates responsibility for an agency's information security. According to FISMA, the CISO is subordinate to the CIO. HHS and its operating divisions adhere to the FISMA requirements, and HHS and each of its operating divisions has a CIO and a subordinate CISO.

Although HHS and its operational divisions comply with these requirements of FISMA, there have been issues regarding the continuity of both CIOs and CISOs. Since 2008, FDA has had six CIOs.[8,9] In addition, FDA was without a permanent CIO from February 2013 to May 2015. During that two-year period, FDA's Deputy Commissioner/Chief Operating Officer also assumed the position of Acting CIO. GAO indicated to committee staff that it is unusual for a federal agency not to have a full-time CIO for more than a year.[10] Similarly, FDA's CISO is still in "Acting" status after filling that role for more than two years.

FDA's lack of permanent IT leadership – in both the CIO and CISO roles – for an extended period raises concerns that the agency is not addressing its key personnel needs for IT with sufficient attention and priority. FDA's threat profile and the concerns noted in the GAO report are troubling due to the importance of FDA's work and the information entrusted to it.

B. Background on the FDA CBER System Breach

[7] FDA's IT budget for fiscal year 2014 was $486 million, which was approximately eleven percent of the total FDA budget of $4.4 billion in fiscal year 2014, a significant investment. *See supra* note 1.

[8] U.S. GOV'T ACCOUNTABILITY OFF., FDA NEEDS TO FULLY IMPLEMENT KEY MANAGEMENT PRACTICES TO LESSEN MODERNIZATION RISKS (GAO-12-346) (Mar. 2012), *available at* http://www.gao.gov/assets/590/589351.pdf

[9] *Meet Todd Simpson, Chief Information Officer*, FDA, June 17, 2015, *available at* http://www.fda.gov/AboutFDA/CentersOffices/ucm451617.htm

[10] E-mail from GAO staff to committee staff, September 8, 2014. One challenge facing the federal government in recruiting IT/cybersecurity professionals is the salary differential. Phyllis Schneck, who recently left the private sector to join the Department of Homeland Security as its Deputy Under Secretary for Cybersecurity, testified during a March 26, 2014 hearing before the Senate Homeland Security and Government Affairs Committee that the difference in pay between the private sector and federal government cybersecurity officials is "six figures before the stock."

On October 15, 2013, an individual gained unauthorized network access to the online submission system of the FDA's Center for Biologics Evaluation and Research (CBER).[11,12] This system maintains the Electronic Biologic Product Deviation Reporting (eBPDR) System, the Electronic Blood Establishment Registration (eBER) System, and the Electronic Human Cell and Tissue Establishment Registration (eHCTERS). The users of these systems are regulated industries, including manufacturers of human cells, tissues, and cellular and tissue based products, and manufacturers of blood and blood components, including transfusion services.

The intruder gained unauthorized access to each registered user's first and last name, the phone number and associated e-mail address, and the username and "hashed" (protected by a specific type of encryption algorithm) password for each account. The CBER Online submission system contained approximately 14,000 current and former user accounts, which corresponded to approximately 12,000 unique users as many users had multiple accounts. Nearly 9,000 of the affected accounts were considered inactive, since they had not been accessed by their account holder since October 17, 2011, or earlier.

FDA discovered the breach on October 15, 2013, the same day that it occurred. Two days later, FDA deactivated the nearly 9,000 accounts that were considered inactive and reset the passwords for the remaining 4,820 active accounts. On October 18, 2013, FDA contacted the active account holders by e-mail and advised them to change their account password. In that e-mail, FDA stated that it had "experienced a technical issue which requires CBER Online users to reset their passwords," and advised that accounts had been assigned a new temporary password.[13] It did not provide additional information on the "technical issue," nor did it contact the inactive account holders to inform them of the need for a password reset at that time.[14]

On November 8, 2013, twenty-four days after the breach was discovered, FDA contacted e-mail holders of active accounts and those whose accounts had been deactivated.[15] In this communication, FDA indicated that the system had been compromised and recommended actions for account holders to take to further protect against fraudulent use of their information. FDA stated that the agency had confirmed that no system data had been altered, and that the

[11] April 7, 2014 letter from FDA Deputy Commissioner for Policy, Planning and Legislation to The Honorable Fred Upton, Chairman, House Committee on Energy and Commerce, *et al*.

[12] When the investigation began, the committee believed that the breach implicated the FDA Electronics Submissions Gateway system. While the Gateway system was not directly compromised, some of the users of the affected CBER systems also possessed accounts for the online submission system and potentially used the same usernames and passwords for both systems. Thus, the information obtained in the breach could have been used by the unauthorized actor to access systems such as the Electronic Submissions Gateway, which housed more sensitive types of data.

[13] E-mail from CBER WebApp Support to FDA/CBER online: Password Reset Required, October 18, 2013. (FDA stated that CBER Online systems covered Blood Establishment Registration, Tissue Establishment Registration and Biological Product Deviation Reporting).

[14] May 6, 2014, briefing with FDA staff. A working assumption in cybersecurity is that most users do not change their passwords unless specifically forced to, and many people reuse usernames and passwords (credentials) across multiple accounts and websites. Thus, the lack of notification received by inactive account holders increased the risks to those users, as the compromised credentials could still be valid for other websites or log-ins. In other words, a clever attacker could use those credentials to access and compromise additional information.

[15] E-mail from CBER WebApp Support to FDA/CBER Online: User Notice, November 8, 2013.

agency continued efforts to confirm that compromised usernames or passwords were not being abused. Soon after these account holders were notified, the breach surfaced in trade press reports.

C. Committee's Investigation into the October 2013 FDA Network Breach

The committee learned of the breach at FDA through the trade press articles that appeared during November 2013. On December 9, 2013, Energy and Commerce Committee Chairman Fred Upton, Oversight and Investigations Subcommittee Chairman Tim Murphy, full committee Chairman Emeritus Joe Barton, full committee Vice Chairman Marsha Blackburn, and Oversight and Investigations Subcommittee Vice Chairman Michael C. Burgess, M.D., launched an investigation into the breach by formally requesting documents and information from FDA. In response to the leaders' request, the committee received documents produced by FDA, obtained background information from federal and industry cyber experts, and conducted interviews with FDA and other personnel.

From information provided in a May 6, 2014 briefing with FDA personnel and a review of key documents, the committee staff learned that the FDA breach was the result of a Structured Query Language (SQL) injection attack. SQL is a programming language used to create and maintain databases and is one of the most popular pieces of software employed by organizations today. SQL databases are used to create tables that organize and track user information such as log-in credentials and personally-identifiable information (PII). Hardware, software, and website applications "query" SQL tables to retrieve this information when, for example, users visit a website and sign into their account.

SQL injection attacks circumvent the SQL programming language syntax in order to bypass security controls that prevent unauthorized users from accessing restricted data. To perform these attacks, a malicious actor inputs a specially formatted query into a user input function such as a search or username bar. The SQL database interprets this query in such a way that it does not perform standard security checks and, in accordance with the specific format of the query and any additional security measures, returns the requested information.

In its December 9, 2013 letter to FDA, the committee also included a request that FDA obtain a third-party audit to assess and ensure the adequacy of their corrective actions. In response to the committee's request, FDA told the committee that it had obtained an independent audit from the Department of Homeland Security's (DHS) United States Computer Emergency Readiness Team (US-CERT).[16] In June 2014, DHS briefed committee staff about the audit.

The audit was a limited assessment of FDA's security system. Due to the nature of the assessment, DHS officials were permitted to assess only the systems to which FDA officials provided access. In addition, FDA officials limited the assessment to seven web applications.[17] Committee staff learned that this was not the first time FDA had imposed limits on the evaluation of their security controls. During a routine examination by OIG into FDA's

[16] April 7, 2014 letter from FDA Deputy Commissioner for Policy, Planning, and Legislation to the Hon. Fred Upton, Chairman, *et al*.
[17] June 5, 2014 briefing with DHS staff.

information security, FDA denied OIG access to seven web applications for reasons of "business criticality." These applications were later found to be vulnerable to SQL injection attacks.

The DHS assessment identified four risk areas; two high-risk, one medium-risk, and one low-risk. DHS made recommendations to address these risks, and FDA stated that it was implementing them. However, FDA stated that it had no timetable for implementation, and it was unclear to committee staff to what extent FDA begun implementation of the DHS recommendations.

While the root cause of the breach was a SQL injection attack, the vulnerability of information on FDA's electronic systems was increased by the linking of the CBER web users table to two additional tables. As a result, the attack compromised all three tables and the information contained within them. Additionally, committee staff learned in the May 6, 2014 briefing that the compromised passwords were not appropriately protected at the time of the breach. FDA's Acting CISO told staff that the passwords were hashed. Hashing algorithms alone is insufficient for password protection. These algorithms, in the absence of a complexity-adding technique known as "salting," are vulnerable to brute-force "guessing" attacks, which can reveal the original password.[18]

FDA's Acting CISO also could not confirm whether the Electronic Submission Gateway (ESG), the website used by industry to submit regulatory information, was encrypted. The protection of the ESG is essential to maintaining the confidence and trust of the regulated companies that are submitting trade secrets and commercial-confidential information. The ESG should have been regarded as a top priority for the Acting CISO, and he should have known whether the ESG was protected by encryption, a widely recommended security control.

Additionally, the PII compromised in the breach had not been encrypted as recommended by Federal security guidance.[19] The encryption process renders confidential data unreadable using advanced mathematics and a secret key. Only those with knowledge of the key can decrypt the data. Encryption provides an additional layer of protection.

FDA also confirmed that the website's underlying "ColdFusion" environment (a web application platform) contributed to the lack of visibility of additional IT issues. Specifically, the Acting CISO said the ColdFusion environment was a legacy system, and was not sure how it was configured or what was in it.[20] The Acting CISO explained that certain portions of the FDA network are owned and operated by contractors, and that the contractors are responsible for the security of those portions. In those cases, FDA's Acting CISO's office has limited authority to

[18] Paul Ducklin, *Anatomy of a password disaster – Adobe's giant-sized cryptographic blunder*, NAKED SECURITY, Nov. 4, 2013, *available at* https://nakedsecurity.sophos.com/2013/11/04/anatomy-of-a-password-disaster-adobes-giant-sized-cryptographic-blunder/.

[19] National Institute of Standards and Technology, U.S. Department of Commerce, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), Recommendations of the National Institute of Standards and Technology, Special Publication 800-122 (2010)(" Organizations can protect the confidentiality of PII at rest, which refers to information stored on a secondary storage device, such as a hard drive or backup tape. This is usually accomplished by encrypting the stored information.").

[20] May 6, 2014 briefing with committee staff.

view or interact with the system.[21] This suggests that FDA cannot protect the contractor-owned and operated portions of its network, nor is it able to access or view those portions of its network.

Internal FDA documents produced in response to the committee's December 9, 2014 letter also revealed that in August 2012, FDA security officials recommended that an FDA system not be accredited. The security assessors found that FDA was operating seven production servers in an unapproved commercial datacenter via an unapproved connection. The security assessor was not permitted to test the physical controls surrounding two commercial data centers, nor was any evidence of an independent assessment provided. The risk surrounding the data centers could not be calculated accurately and was found to be a high risk to the enterprise due to the level of unknowns. The same assessment identified nine high risk and twenty medium risk vulnerabilities. These were in addition to eleven medium risk vulnerabilities identified in previous assessments. Despite these findings, FDA's CIO argued that appropriate system security controls were properly implemented and that a satisfactory level of security was present.[22]

D. Committee Staff's Analysis of FDA's Response to the CBER System Breach

According to the Open Web Application Security Project (OWASP), considered a standard for web security,[23] SQL injections have been a top web vulnerability for several years. IT and security personnel can remove the risk of SQL injection attacks by including a step in the querying process to "sanitize" user-inputted data before it is submitted to the database. This step, often implemented as a few additional lines of code in the querying routine, examines the user-inputted data and strips out the special characters on which SQL injection attacks rely. Without those special characters, the SQL attacks fail.

In an interview with committee staff, FDA's Acting CISO acknowledged that SQL injections are relatively trivial attacks that a malicious actor with low-level skills can use to exploit a public-facing website. When asked why the CBER application lacked protection against such attacks, the Acting CISO told committee staff that the Intrusion Detection System (IDS) on which his office relies did not scan "deep enough" into the system. He explained, the IDS did not perform, and had not performed, a security scan on that portion of the system for an unidentified amount of time. Until the October 2013 breach, the information security office had remained under the impression that its IDS protected the entirety of their network. The FDA officials who were responsible for the security of FDA's network did not understand nor have full visibility into the internal behavior of their own network.

With a $486 million IT budget, FDA had the resources to prevent SQL injection attacks. One computer security expert, talking on background with committee staff, characterized the failure to protect against SQL injections as the equivalent of "leaving the front door open." Despite

---

[21] *Id*.
[22] May 1, 2014, in-camera review of FDA documents.
[23] *National & International Legislation, Standards, Guidelines, Committees and Industry Codes of Practice*, OPEN WEB APPLICATION SECURITY PROJECT, *available at* https://www.owasp.org/index.php/Industry:Citations#National_.26_International_Legislation.2C_Standards.2C_Guidelines.2C_Committees_and_Industry_Codes_of_Practice.

understanding the risks of SQL injections and having the means with which to thwart them, FDA did not take adequate steps to prevent the breach.

The inability of FDA to mitigate even this type of low-level threat raises the troubling questions about FDA's preparedness for more sophisticated, and more dangerous, cyber threats.[24] The failure by FDA to take adequate action against the known threat of SQL injections may not have violated any federal law, regulation, or standard, but it appears to be the result of poor security management and an example of a control deficiency that places agency data at an increased and unnecessary risk of unauthorized access, disclosure, and misuse.

E. The Lauri Love Case

Less than two weeks after the October 2013 FDA breach, two U.S. Attorney offices issued press releases announcing criminal charges against an alleged malicious actor who compromised information systems at multiple federal agencies. This actor allegedly deployed SQL injection attacks against the agency systems, either alone or in conjunction with exploits that targeted vulnerabilities in ColdFusion environments. The similarity of these attacks to the breach at FDA suggested possible linkage to the issues the committee was already examining, as the announcements indicated that several of the attacks affected additional HHS operating divisions.

On July 24, 2014, Lauri Love of Stradishall, England, was indicted by a federal grand jury in the Eastern District of Virginia on charges of conspiracy, causing damage to a protected computer, access device fraud, and aggravated identity theft related to the breaching of multiple government computers.[25] According to the indictment, on or about December 24, 2012, Love allegedly uploaded without authorization hacking tools known as backdoor shells to the domains ask.hrsa.gov and accessdata.fda.gov. Although no specific overt act was linked to the NIH, the grand jury indictment issued by the U.S. Attorney for the Eastern District of Virginia listed NIH, the Health Resources and Services Administration (HRSA), and FDA as HHS operating divisions affected by Love's actions.[26] The indictment stated that Love and his conspirators gained unauthorized access to the protected computers that hosted the websites by exploiting a vulnerability in Adobe ColdFusion. The vulnerability allowed the malicious actors to bypass security on protected computers without authorization.

---

[24] For example, Chinese cyberespionage actors are targeting the healthcare and medical/life sciences industries. Researchers also have tied Chinese hackers to an attack that targeted the National Institutes of Health. Kelly Jackson Higgins, Medical Industry Under Attack by Chinese Hackers, darkreading.com, (2013).

[25] The press release about the indictment alleged that Love unlawfully obtained massive amounts of sensitive and confidential information stored on breached government computers, including more than 100,000 employee records with names, Social Security numbers, addresses, phone numbers, and salary information, along with more than 100,000 financial records, including credit card numbers and names. Love's actions allegedly caused total losses in excess of $5 million. However, it appears that these impacts were related to breaches of government agency computers outside of HHS.

[26] In a June 26, 2014 briefing with committee staff, the HHS CISO said that incidents at HRSA and on December 24, 2012, were actually one incident. The compromised data belonged to HRSA, but was hosted by NIH as a service provider for the network.

With respect to the alleged HRSA breach, the HHS OIG and the HHS Acting CISO confirmed that the HRSA system was infected on December 24, 2012.[27] The exploit used was designed to gain access to databases and passwords, but was not successful. As a precautionary measure, HRSA changed all database passwords related to ask.hrsa.gov on January 4, 2013. Using the information about the breach, HRSA checked all of its other systems and found no evidence of additional infections. The ask.hrsa.gov system was retired this year and no longer exists. As part of its response to committee staff's request for additional information on the incident, HRSA provided contact information for the OIG special agent involved in the Love case investigation.

With respect to the alleged NIH incident, the committee received conflicting and confusing information. Initially, NIH confirmed the December 24, 2012 breach reported in the October 2013 press release from the U.S. Attorney's Office for the Eastern District of Virginia. NIH reported to committee staff that NIH detected the intrusion in progress and interrupted further activity. The root cause was identified as a SQL injection and corrected. NIH subsequently searched its systems for similar vulnerabilities and corrected issues before they became active.[28] According to NIH staff, the source of this information was the NIH CISO, who retired at the end of June 2014.[29]

Per standard NIH and HHS operating procedure, NIH reported the December 2012 incident to HHS' Computer Security and Incident Response Center (CSIRC), which shares information with OIG and US-CERT.[30] According to HHS OIG, the NIH Incident Response Team (IRT) supplied information to its office that contributed to the criminal investigation. In an October 2013 e-mail, the OIG agent thanked the NIH CISO and the NIH Deputy CISO for their assistance.[31]

However, during an August 22, 2014 briefing to further discuss this breach, NIH denied that there was an incident involving HRSA data hosted on NIH servers, denied that there was an incident in December 2012, and denied that there was an NIH security incident involving SQL injections. In an e-mail subsequent to the briefing, NIH stated that the reference to SQL injections was included in an earlier response in error.[32] NIH stated, "We apologize for any confusion this may have caused."[33] The briefers were the NIH CIO and the NIH Acting CISO, who had been the Deputy CIO at NIH at the time of the incident.

During the briefing, NIH representatives stated that the October 2013 Department of Justice press release referenced an NIH security incident related to Adobe ColdFusion that was identified, remediated, and reported by NIH in March 2013. The breach did not result in the compromise of any user accounts or the loss of NIH data. The affected server did not contain sensitive information or user accounts. NIH's IDS detected and automatically blocked the actors when they attempted to establish a connection between the NIH server and their location, thereby

[27] E-mail from Director of Legislation, HRSA to committee staff, October 10, 2014.
[28] E-mail from NIH Office of Legislative Policy and Analysis (OPLA) to committee staff, June 26, 2014.
[29] Conference call with NIH staff, August 22, 2014.
[30] E-mail from NIH OPLA to committee staff, June 23, 2014.
[31] NIH later clarified that the assistance was related to providing technical forensic information specific to the Adobe ColdFusion incident that contributed to the criminal case.
[32] E-mail from NIH OLPA to committee staff, August 26, 2014.
[33] *Id.*

preventing them from removing NIH data. NIH performed a number of activities to assess and remediate the situation, following established procedures for these types of incidents.

Committee staff sought clarification about the March 2013 incident described by NIH, and OIG reported that there were in fact two security incidents on the NIH network. The first incident took place in December 2012, and was the breach referred to in the indictment. The other incident took place in March 2013, and was first described by NIH during the August 2014 briefing. OIG indicated that the March 2013 incident identified by NIH as one incident was, in fact, two separate and unrelated intrusions and acts of separate subjects, one of whom was Love. OIG and its investigative partners subsequently determined that Love's intrusion at NIH occurred at approximately the same time as an intrusion at HRSA, on or about December 24, 2012. Further, OIG confirmed that there was no exfiltration as part of the December 24, 2012 intrusion[34] or the intrusion involving the non-Love intrusion in March 2013.[35]

In contrast to HRSA and NIH, FDA's Acting CISO told committee staff that the agency did not know in real-time about the breach on December 24, 2012, and insisted that he was not aware of such an incident when it happened or even after the grand jury indictment was reported in July 2014. Further, he informed committee staff that FDA could not find any evidence that this breach ever occurred and stated that "nothing happened in [the FDA] environment" on December 24, 2012.

Given FDA's insistence and doubts about evidence of the existence of the December 24, 2012, incident, committee staff challenged HHS OIG about the breach. OIG stood by its finding that there was a December 24, 2012 breach of FDA's systems. Further, OIG reported that, in coordination with investigative partners, it determined that the FDA intrusion was related to the HRSA and NIH intrusions by Love.

F. Briefing with HHS Officials to Discuss Findings

In a subsequent briefing about FDA's findings – including information from the Love indictments – the FDA Acting CISO addressed committee staff concerns about the lack of protections in FDA networks from SQL injections, stating that his team does not look at specific code present in the system, but instead relies on vulnerability tools. He explained that his office does not have the resources to perform Quality Assessment checks on contractor code, which may have been the vulnerability exploited by the SQL attacks. To address this area of risk in the aftermath of the October 2013 breach, the FDA's Acting CISO introduced additional capabilities into the FDA network that include supplementary and more robust vulnerability scanners.

FDA's Acting CISO also addressed concerns about the lack of visibility FDA officials have in regards to legacy systems and contractor-owned and operated portions of the networks. Contrary to the impression given during the May 6, 2014 briefing, the Acting CISO denied that the office suffers from visibility issues in regards to legacy systems, and stated that the office could obtain visibility into contractor-owned and operated portions of the FDA network when necessary.

[34] E-mail from HHS OIG staff to committee staff, September 30, 2014.
[35] E-mail from HHS OIG staff to committee staff, October 6, 2014.

In response to committee staff concerns about threat-intelligence coordination by HHS among its operating divisions, HHS's Acting CISO stated in a June 26, 2014 briefing that HHS had modified its threshold-alert policy. An alert is now sent out department-wide in the case of a single incident involving an HHS agency. The previous practice had been to send out an alert when there were incidents at a minimum of five operating divisions.[36]

PART II – ADDITIONAL HHS INCIDENTS

A. Breach of the Substance Abuse and Mental Health Services Administration (SAMHSA) Website

The committee's investigation began with the October 2013 breach at FDA and later expanded to include the December 2012 breaches at FDA, HRSA, and NIH. These incidents suggested inadequate information security at HHS as a whole, and the committee subsequently widened its investigation to include the information security programs of all HHS operating divisions.

In the course of the investigation, committee staff discovered an article from *The Weekly Standard* published October 3, 2013, that stated that a subdomain administered by the Substance Abuse and Mental Health Services Administration (SAMHSA) had been advertising items such as NFL jerseys and UGG boots.[37] Staff contacted HHS OIG on November 25, 2014, to request more information about the incident.

Through a series of e-mails in December 2014, OIG informed committee staff that HHS had identified the vulnerability used against the SAMHSA subdomain and had taken action to address the issue.[38] When pressed to disclose the vulnerability, OIG stated that its role was limited to the initial investigation into the actions of the malicious actor, and it was unable to provide further details on the incident itself. OIG suggested that committee staff speak with HHS' CSIRC or with SAMHSA for more information.[39]

Committee staff contacted the HHS CSIRC on December 15, 2014, with a request to provide additional information on the security incident. A representative of HHS's Office of the Assistant Secretary for Legislation (ASL) responded on December 18, 2014, stating that forensic analysis provided by SAMHSA confirmed that a web server had been compromised.[40] SAMHSA did not specify what vulnerability was exploited. In addition, committee staff were told that SAMHSA's analysis uncovered a text file placed on the server by the malicious actor. This file allegedly

---

[36] Staff notes, Briefing with HHS Acting CISO and HHS Deputy CISO, June 26, 2014, and Briefing with HHS Acting CISO and CSIRC Director, October 22, 2014.

[37] Jeryl Bier, *HHS-Run Website Hacked; Now Selling NFL Jerseys, Ugg Boots, Armani Fragrances*, THE WEEKLY STANDARD, Oct. 13, 2013, *available at* http://www.weeklystandard.com/blogs/hhs-run-website-hacked-now-selling-nfl-jerseys-ugg-boots-armani-fragrances_759213.html.

[38] E-mail from HHS OIG Director of Congressional and Regulatory Affairs to committee staff, December 15, 2014.

[39] According to information received as part of the committee's investigation, OIG was responsible for the "criminal" aspects of the SAMHSA breach investigation, while CSIRC and SAMHSA were responsible for the incident investigation and remediation.

[40] E-mail from HHS Office of the Assistant Secretary for Legislation to committee staff, December 18, 2014.

contained the actor's signature and a list of vulnerabilities that the actor claimed to have used against the web server. Both OIG and CSIRC closed their investigations into the incident on May 21, 2014, due to a lack of evidence.[41]

Committee staff requested a copy of the text file containing the list of vulnerabilities, as well as the initial date of compromise and date of remediation. According to the response received on January 6, 2015, from HHS ASL, the web server was compromised on October 3, 2013, and the infection was remediated the same day.[42] The HHS ASL also provided a copy of the list of vulnerabilities, although he did not include a copy of the original text file left by the malicious actor.[43]

In a follow-up e-mail on January 27, 2015, the HHS ASL clarified that the web server infection had been remediated on October 4, 2013, the day after the initial infection. He also identified the vulnerability used to exploit the server as a Cross-Site Scripting (XSS) attack.[44] XSS attacks are similar to SQL injection attacks in that they use website input functions such as search bars to "inject" malicious code into an otherwise benign web service. They also are similar to SQL injection attacks in that the risks of XSS attacks may be mitigated using data "sanitization."[45]

With regard to the list provided by HHS ASL on January 6, 2015, research and analysis conducted by committee staff revealed several discrepancies. First, the list did not contain vulnerabilities, but aliases used by hackers. Second, while this list was presented as evidence related to the October 3, 2013 compromise in which a SAMHSA subdomain was used to conduct malicious advertising, the existence of the text file and its content suggests that the list was related to a separate security incident.

Malicious advertising attacks such as the one suffered by SAMHSA usually are performed by automated scans that search the Internet for exploitable vulnerabilities in networked devices.[46] When a vulnerable device is found, the scan exploits the device and "commandeers" the website for the purposes of malicious advertising.

These scans usually do not deliver text files such as the one discovered by the SAMHSA information security team. Instead, these types of text files typically are left as "calling cards" by malicious actors who exploit vulnerable sites in order to spread a message or to obtain bragging rights. Considering that the text file contained the names of several members of an online hacking forum,[47] it is likely that the text file was left by a malicious actor who compromised the

---

[41] *Id.*
[42] E-mail from HHS Office of the Assistant Secretary for Legislation to committee staff, January 6, 2015.
[43] *Id.*
[44] E-mail from the HHS Office of the Assistant Secretary for Legislation to committee staff, January 27, 2015.
[45] *Cross-site Scripting (XSS)*, THE OPEN WEB APPLICATION SECURITY PROJECT, Apr. 22, 2014, *available at* https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29.
[46] *Crawling & Indexing*, GOOGLE, *available at* https://www.google.com/search/about/insidesearch/howsearchworks/crawling-indexing.html (last visited May 28, 2015).
[47] Harry Misiko, *How Anonymous and other hacktivists are waging war on Kenya*, THE WASHINGTON POST, July 30, 2014, *available at* http://www.washingtonpost.com/blogs/worldviews/wp/2014/07/30/how-anonymous-and-other-hacktivists-are-waging-war-on-kenya/.

SAMHSA site, on or around the same date and using a similar vulnerability, as the automated scan. Given this inconsistency, there is reason to believe that SAMHSA suffered two information security compromises on or around October 3, 2013.

B. Additional Information Security Concerns

Additional incidents came to the attention of committee staff during review of information security incidents at HHS and its operating divisions.

1. Compromise of Federally Facilitated Marketplace Testing Server By Automated Scan

On August 25, 2014, federal officials discovered malware on a testing server within the Federally Facilitated Marketplace (FFM) network, which contains the infrastructure used to run the website www.HealthCare.gov.[48] The subsequent investigation concluded that the compromise resulted from an automated scan used by malicious Internet actors to find and exploit vulnerable networked devices, and that the scan succeeded because the testing server had been misconfigured.

In a briefing with committee staff, CMS' CIO identified the three misconfigurations that led to the compromise: an external-facing Internet Protocol (IP) address, which permitted communication between the testing server and the general Internet; the use of default credentials, which allowed the scan to "guess" the username and password needed to gain privileged access to the server; and the absence of a security scan, which prevented CMS officials from identifying these vulnerabilities.[49] While the malware placed on the system was considered low-risk and no system data was exposed, the accidental misconfiguration and subsequent compromise of a server within CMS FFM networks further highlights the weaknesses inherent in HHS information security.

2. OIG Auditors Gained Remote Access to Indian Health Service Server

In June 2013, HHS OIG performed an assessment of the Indian Health Service (IHS) network and associated information systems.[50] During that assessment, OIG auditors were able to gain unauthorized, remote access to an IHS web server through the exploitation of a critical, unpatched, unmitigated vulnerability. With that access, the auditors were able to obtain user credentials from the server, as well as to make changes to the server's configuration. They also were able to obtain usernames and passwords from IHS databases connected to the compromised server.[51]

Had the compromise been executed by a malicious actor instead of OIG, that actor could have used their unauthorized, remote access to place malware on the network, expose the PII of IHS

---

[48] Danny Yadron, *Hacker Breached HealthCare.gov Insurance Site*, WALL ST. J., Sept. 4, 2014, *available at* http://online.wsj.com/articles/hacker-breached-healthcare-gov-insurance-site-1409861043.
[49] Briefing with committee staff and CMS CIO, September 10, 2014.
[50] DEPT. OF HEALTH AND HUMAN SERVICES, OFF. OF INSP. GEN., THE INDIAN HEALTH SERVICE'S NETWORK SYSTEMS WERE AT HIGH RISK OF COMPROMISE BY CYBER ATTACKS (A-18-13-30330) (Jan. 2014).
[51] *Id.*

patients and employees, or otherwise negatively impact IHS's ability to perform its duties. The OIG report stated that the leveraged vulnerability had been exploitable for several months prior to the audit. This implies that a significant timeframe existed wherein an outside, malicious actor could have breached the IHS network, though OIG did not determine whether or not such a compromise had occurred.

3. State of Information Security at the Office of the Secretary Risks Significant Data Breaches

In April 2012, HHS OIG released a non-public report entitled "Weak Network Management Controls at the Office of the Secretary Poses Risk of Significant Data Breaches Occurring and May Severely Impact Critical Operations and the Mission of Health and Human Services."[52] The report examined controls for the Office of the Secretary (OS) and the Information Technology and Infrastructure Operations Office (ITIO)[53] and found that "the network management controls over the OS's network were inadequate and in need of improvement." OIG auditors identified thirty-nine reportable exceptions that they consolidated into seven findings, five of which were considered "high risk." As such, OIG stated that "[OIG] believes the current state of information security at OS poses the risk of significant data breaches occurring and may even severely impact critical operations and the mission of HHS."[54]

Recent audits by OIG reveal that many of the deficiencies identified in the 2012 OIG report remain unresolved. In January 2015, OIG released a report on OS's compliance with the FISMA.[55] They also released a report in December 2014 that examined information security controls at ITIO.[56] In the January 2015 report, OIG found that three of the five "high risk" findings cited in the April 2012 report had not been addressed adequately by OS. ITIO was no better – in fact, it was worse. OIG once again cited ITIO for four of the five "high risk" findings. Though both reports detail improvements from the April 2012 report in which OIG stated that information security at OS posed the risk of significant data breaches, the reoccurrence of several "high risk" findings three years later at OS and ITIO show that information security at both offices remains inadequate.

C. Information Security Deficiencies at HHS and its Operating Divisions

Though the security incidents detailed throughout this report resulted in relatively minor exploitations, the susceptibility of FDA, NIH, HRSA, SAMHSA, CMS, and IHS networks to

---

[52] DEPT. OF HEALTH AND HUMAN SERVICES, OFF. OF INSP. GEN., WEAK NETWORK MANAGEMENT CONTROLS AT THE OFFICE OF THE SECRETARY POSES RISK OF SIGNIFICANT DATA BREACHES OCCURRING AND MAY SEVERELY IMPACT CRITICAL OPERATIONS AND THE MISSION OF THE HEALTH AND HUMAN SERVICES (A-18-11-30250) (Apr. 2012).

[53] The ITIO office provides enterprise network and security infrastructure services to HHS staff divisions and smaller HHS operating divisions.

[54] *See supra* note 52.

[55] DEPT. OF HEALTH AND HUMAN SERVICES, OFF. OF INSP. GEN., REVIEW OF THE OFFICE OF THE SECRETARY'S COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002 FOR FISCAL YEAR 2014 (A-18-14-30320) (Dec. 2014).

[56] DEPT. OF HEALTH AND HUMAN SERVICES, OFF. OF INSP. GEN., THE INFORMATION TECHNOLOGY INFRASTRUCTURE AND OPERATIONS OFFICE HAD INADEQUATE INFORMATION SECURITY CONTROLS (A-18-14-30420) (Jan. 2015).

minor, well-known, and preventable exploits such as SQL injections, XSS attacks, default credential exploitation, and automated scanning is troubling. The diversity of the agencies, officials, networks, technologies, and exploits involved in these incidents suggest that no individual official or technology is to blame. Rather, there is a fundamental weakness within the information security programs in place at HHS and its operating divisions.

To further investigate this concern, the committee sent a document request letter to the HHS OIG to obtain several non-public reports pertaining to HHS information security.[57] These reports included annual FISMA compliance audits, as well as additional non-FISMA audits. Committee staff requested the most recent FISMA and non-FISMA audit reports available for each operating division.

Individually, these audits highlight the numerous information security deficiencies that exist within each respective operating division's information security program. Taken as a whole, the pervasive shortcomings within these information security programs demonstrate a fundamental weakness in HHS's approach to information security. As seen in Table 1 and Table 2, not only does each division suffer from numerous information security deficiencies, in many cases, they suffer from nearly identical deficiencies, suggesting that HHS's information security program, and those of its operating divisions, are flawed.

Table 1 - HHS OIG Non-FISMA Audit Reports

Operating Division	Year	Inventory Management	Patch Management	Antivirus Management	Logical Access Controls	USB Controls	Outdated/Unauthorized Operating System Software	Full (Whole) Disk Encryption	Website Vulnerabilities	Configuration Management	Security Event Management/Incident Response	Security Management Infrastructure	Encryption	Security Program Oversight
SAMHSA[58]	2012	X	X	X	X	X								
OS[59]	2011	X^R	X^R	X^R	X^R		X^R	X^R	X					
ITIO[60]	2013	X	X	X	X	X				X				
IHS[61]	2012	X	X	X	X		X			X	X	X		
FDA[62]	2011	X	X	X	X		X		X				X	

[57] January 20, 2015, letter from the Honorable Fed Upton, Chairman, Energy and Commerce Committee, and the Honorable Tim Murphy, Chairman, Oversight and Investigations Subcommittee, to the Honorable Daniel Levinson, HHS OIG.

[58] DEPT. OF HEALTH AND HUMAN SERVICES, OFF. OF INSP. GEN., INFORMATION SECURITY WEAKNESSES POSES RISK TO OPERATIONS AND THE MISSION OF THE SUBSTANCE ABUSE AND MENTAL HEALTH SERVICES ADMINISTRATION (A-18-12-30420) (SEPT. 2013).

[59] *See supra* note 52.

[60] *See supra* note 55.

[61] *See supra* note 50.

[62] DEPT. OF HEALTH AND HUMAN SERVICES, OFF. OF INSP. GEN., CONTINUING INFORMATION SECURITY WEAKNESSES POSE RISK TO OPERATIONS AND THE MISSION OF THE FOOD AND DRUG ADMINISTRATION (A-18-11-30330) (Jun. 2012).

AHRQ[63]	2011	X	X	X			X			X				X

Note: An "R" denotes a repeat finding from the previous year's audit report.

Table 2 - HHS OIG FISMA Audit Reports

Operating Division	Year	Access and Identity Management	Configuration Management	Information Security Governance	Security Training	Plans of Action And Milestones	Network Management	Continuous Monitoring	Risk Management	Remote Access Management	Contingency Planning	Security Planning	Incident Response	Contractor Oversight
Department[64]	2008	X	X	X	X	X	X							
FDA[65]	2013	X^{R}	X^{R}		X	X^{R}		X	X^{R}	X^{R}	X^{R}	X^{R}		
NIH[66]	2014		X			X		X	X		X	X	X	X
OS[67]	2014	X^{R}	X^{R}		X^{R}	X^{R}		X^{R}	X^{R}	X^{R}	X^{R}	X^{R}	X	X^{R}
CDC[68]	2012		X						X			X		
CMS[69]	2014	X^{R}	X^{R}		X^{R}	X^{R}		X^{R}	X^{R}	X^{R}	X		X^{R}	

Note: An "R" denotes a repeat finding from the previous year's audit report.

As Table 1 shows, each of the six non-FISMA-audited operating divisions was deficient in inventory, patch, and antivirus management. This is especially troubling because a website vulnerability and a missing patch led to the FDA and IHS[70] compromises, respectively. Likewise, Table 2 shows that each of the six FISMA-audited operating divisions was deficient in configuration management, the root cause of the FFM server and FDA compromises. In both Table 1 and Table 2, several information security deficiencies cited in the audit reports were repeat findings from previous years.

[63] DEPT. OF HEALTH AND HUMAN SERVICES, OFF. OF INSP. GEN., OPPORTUNITIES EXIST TO STRENGTHEN INFORMATION SECURITY CONTROLS AT THE AGENCY FOR HEALTHCARE RESEARCH AND QUALITY (A-18-11-30220) (Dec. 2011).

[64] DEPT. OF HEALTH AND HUMAN SERVICES, OFF. OF INSP. GEN., AUDIT OF THE DEPARTMENT'S SECURITY PROGRAM (A-18-08-30140) (Sept. 2008).

[65] DEPT. OF HEALTH AND HUMAN SERVICES, OFF. OF INSP. GEN., REVIEW OF THE FOOD AND DRUG ADMINISTRATION'S COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002 FOR FISCAL YEAR 2013 (A-18-13-30440) (Feb. 2014).

[66] DEPT. OF HEALTH AND HUMAN SERVICES, OFF. OF INSP. GEN., REVIEW OF THE NATIONAL INSTITUTES OF HEALTH'S COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002 FOR FISCAL YEAR 2014 (A-18-14-30270) (Dec. 2014).

[67] *See supra* note 55.

[68] DEPT. OF HEALTH AND HUMAN SERVICES, OFF. OF INSP. GEN., U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES, CENTERS FOR DISEASE CONTROL AND PREVENTION, FEDERAL INFORMATION SECURITY MANAGEMENT ACT PROGRAM AUDIT FOR FISCAL YEAR 2012 (A-04-12-05041) (Jan. 2013).

[69] DEPT. OF HEALTH AND HUMAN SERVICES, OFF. OF INSP. GEN., REVIEW OF THE CENTERS FOR MEDICARE & MEDICAID SERVICES' COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002 FOR FISCAL YEAR 2014 (A-18-14-30310) (Dec. 2014).

[70] The IHS network was compromised during an audit performed under controlled conditions by HHS OIG. However, the vulnerability that permitted the compromise had been exploitable for several months prior to the OIG test and OIG did not determine whether outside malicious actors had already compromised the server.

Overall, the audits summarized in Tables 1 and 2 support the committee's concern that a fundamental weakness exists in HHS and its operating divisions' information security programs. This weakness lies at the core of the pervasiveness and persistence of the information security deficiencies cited in the audits, and places the valuable information held by HHS and its operating divisions at increased risk of exposure and compromise. Throughout the committee's investigation, the subordination of information security concerns in favor of operational concerns has been a consistent weakness at HHS and its operating divisions.

PART III – OBSERVATIONS

A. Information Security Subordination Across HHS and its Operating Divisions

The committee's investigation found several incidents in which information security concerns were explicitly subordinated to operational concerns:

1. HHS OIG Denied Access to Seven Web Applications During 2013 FDA Security Audit

As part of the investigation into the October 2013 compromise at FDA, committee staff examined an audit OIG performed of FDA's information systems in the fall of 2013.[71] OIG auditors were denied access to seven web applications within the FDA network during this audit, a finding which they noted violated the *HHS Office of the Chief Information Officer's Policy for Information Systems Security and Privacy Handbook*.[72] This policy requires HHS's operating divisions to assess the security controls in information systems annually. FDA's Acting CISO restricted access to the applications due to their "business criticality," as FDA officials were concerned that the security testing performed as part of the audit would negatively impact FDA regulatory activities and business operations. The restricted applications included the CBER application, which was breached in the October 2013 incident. As part of their internal investigation, HHS Officials discovered, and FDA's Acting CISO later disclosed to committee staff, that each of these web applications was vulnerable to SQL injection attacks,[73] the exploit used in the October 2013 breach and a vulnerability that the OIG audit identified in FDA web pages to which they were granted access.[74]

2. "Authority to Operate" Given to the Federally Facilitated Marketplace In Spite of Incomplete Security Control Assessment

The Patient Protection and Affordable Care Act (PPACA) mandated the development and deployment of a web-based system through which Americans could purchase health insurance, known as the Federally Facilitated Marketplace (FFM). CMS was designated as the responsible authority for the FFM. To comply with federal regulations related to information security, the

[71] *See supra* note 1.
[72] Conference call with HHS OIG Audit team, October 23, 2014.
[73] May 6, 2014 briefing with committee staff.
[74] Conference call with HHS OIG Audit team. October 23, 2014.

FFM and its component systems underwent four Security Control Assessments (SCAs) conducted by information security corporation MITRE prior to its launch on October 1, 2013. MITRE was unable to complete the final SCA of the Health Insurance Exchange component of the FFM, as incomplete systems and applications forced CMS officials to limit the scope of the assessment. In recognition of the risks associated with launching the site in spite of the incomplete SCA, the CMS CIO put in place a mitigation plan and recommended that the CMS Administrator issue the FFM an "Authority to Operate" (ATO) after being informed of those risks. In a Decision Memorandum, the CMS CIO acknowledged that the compensating mitigation plan did not "reduce the risk to the FFM system itself going into operation on October 1, 2013."[75] The CMS Administrator accepted the recommendation of the CMS CIO and issued a six-month ATO, acknowledging in a signed memorandum that federal regulations required that the FFM "successfully undergo a Security Control Assessment (SCA)" and that "[d]ue to system readiness issues, the SCA was only partly completed."[76] The ATO allowed the FFM to go forward with a mitigation plan in place and to perform a "complete SCA" in the intervening period. Without attributing it to any particular factor, committee staff note that nine months later, an automated scan compromised the FFM and placed malware within the network.

3. Office of Civil Rights Focused On "System Operability to the Detriment of System and Data Security"

In a November 21, 2013 audit of the HHS Office of Civil Rights (OCR), HHS OIG noted that OCR was not fully complying with federal information security requirements. In particular, OIG stated that, "OCR management focused on the operability of the systems . . . and did not focus on securing the systems used to store, retrieve, process, and track Security Rule oversight and enforcement data."[77] Further, OCR "focused on system operability to the detriment of system and data security."[78] As OCR is responsible for enforcing compliance with health information privacy and security laws, the data that it holds as a result of its oversight is valuable. OCR's focus on operational concerns over security concerns, as noted by OIG, places that data at increased risk of exposure or misuse.

B. Identified Vulnerabilities within HHS and Its Operating Divisions' Information Security Programs

This operational prioritization has resulted subordination of security concerns. It also has resulted in adverse secondary effects to the overall adequacy of information security programs at HHS and its operating divisions. The committee's investigation revealed several issues that raised questions as to whether or not information security personnel have the appropriate

[75] "Federal Facilitated Marketplace Decision Memo Risk Acknowledgment Signature Page," signed: T. Fryer, T. Trenkle, M. Snyder, dated: September, 27, 2013.
[76] "Federal Facilitated Marketplace Decision Memo Risk Acknowledgment Signature Page," signed: M. Tavenner, dated: September, 27, 2013.
[77] DEPT. OF HEALTH AND HUMAN SERVICES, OFF. OF INSP. GEN., THE OFFICE OF CIVIL RIGHTS DID NOT MEET ALL FEDERAL REQUIREMENTS IN ITS OVERSIGHT AND ENFORCEMENT OF THE HEALTH INSURANCE AND PORTABILITY AND ACCOUNTABILITY ACT SECURITY RULE at 7 (A-04-11-05025) (Nov. 2013).
[78] *Id* at 4.

authorities and expertise necessary to carry out their duties, including:

(1) Audits of information security at two operating divisions were constrained due to operational concerns and incompleteness. In both cases, the CIO-CISO hierarchy prevented the CISO from completing full system audits.

(2) Information security officials are not always permitted full visibility into their own networks as a result of their relationship with agency contractors, who may own and operate portions of agency networks.

(3) Two information security breaches at two different operating divisions resulted from misconfigurations. A separate breach resulted from a missing "critical" software patch. These incidents call into question whether information security officials have the appropriate level of expertise.

(4) The information security officials at one operating division misidentified a list of hacker aliases as a list of security vulnerabilities.

(5) Officials at two operating divisions were unable to provide accurate information about security incidents within their own networks.

Committee staff believe that the operational prioritization exhibited by officials at HHS and its operating divisions contributes to the lack of appropriate authorities and expertise within their information security programs.

The information security incidents and ongoing troubles with information security across HHS and its operating divisions raise the question as to why officials at different agencies, operating and securing technologically unique networks, are consistently making similar decisions in regards to the operation and security of those networks. It suggests a flaw in the structure of information security offices and positions at HHS and its operating divisions. Evidence from the committee's investigation suggests that the tendency to subordinate security concerns to operational concerns stems from the organizational relationship and division of authorities between the CIO and the CISO.

C. Security as an Operational "Release Valve"

Currently, the top agency official for information security at HHS is the CIO. However, information security is neither the only nor the primary objective of that office. In addition to information security, the CIO also is responsible for the development, implementation, management, and operation of IT across HHS.[79] FISMA requirements and department policy delegate routine information security responsibilities to the HHS CISO. However, final approval

[79] *What We Do*, U.S. DEPT. OF HEALTH AND HUMAN SERVICES, *available at* http://www.hhs.gov/ocio/about/whatwedo/what.html.

for information security actions and expenditures remains with the CIO.[80] This organizational structure subordinates information security to information operations, placing information security at a severe disadvantage.

Other federal agencies have struggled with the challenge of balancing operational objectives with security or safety concerns. For example, the lessons learned in the aftermath of the Challenger and Columbia shuttle disasters illustrated the consequences of prioritizing operations to the detriment of security. The House Committee on Science and Technology found in their report on the Challenger accident that "[t]he pressure on NASA to achieve planned flight was so pervasive that it undoubtedly adversely affected attitudes regarding safety."[81] Similarly, the Columbia Accident Investigation Board highlighted the fact that "NASA had conflicting goals of cost, schedule, and safety. Safety lost out as the mandates of an 'operational system' increased the schedule pressure."[82]

As the pressure to create a sustainable, reliable, and operational shuttle system grew, managers at NASA and relevant contracting firms responded by "normalizing deviance."[83] Authorities responsible for the shuttle program chose to accept greater and greater safety risks to meet operational goals – contributing to the eventual loss of the Challenger, the Columbia, and their crews.

Recent information security compromises at HHS have proven that this same dilemma exists for HHS and its operating divisions today. When IT security concerns and operational needs clash – as they did when FDA officials limited the scope of the OIG audit, when CMS officials decided to launch the FFM in spite of incomplete security testing, and when OCR chose to prioritize systems operability over security – operational needs are prioritized and security concerns downplayed, delayed, or ignored. IT is critical to the business operations and regulatory activities of HHS, but information security at HHS has yet to reach a maturity level comparable to that of IT operations.

When asked to comment on this slow development, industry CISOs and experts with whom committee staff spoke on background agreed that the CIO-CISO hierarchy and the subordination of security to operations are likely primary factors. They explained that an analogous situation exists for many industry organizations whose information security apparatus is combined with or subordinated to their operations apparatus. One CISO described an experience where a CIO refused to purchase an advanced security product for three consecutive years, though company customers had requested the product, in order to expand and update operational capabilities. This

[80] *HHS-OCIO-2011-0003*, DEPT. OF HEALTH AND HUMAN SERVICES, http://www.hhs.gov/ocio/policy/hhs-ocio-2011-0003.html#_Toc297638397
[81] STAFF OF H. COMM. ON SCIENCE AND TECHNOLOGY, 99TH CONG., INVESTIGATION OF THE CHALLENGER ACCIDENT (COMM. PRINT 1986) at 130, *available at* http://www.gpo.gov/fdsys/pkg/GPO-CRPT-99hrpt1016/pdf/GPO-CRPT-99hrpt1016.pdf.
[82] ROBERT GODWIN, COLUMBIA ACCIDENT INVESTIGATION BOARD: REPORT 200 (Apogee Books 2003) (2003), *available at* http://anon.nasa-global.speedera.net/anon.nasa-global/CAIB/CAIB_lowres_chapter8.pdf.
[83] *Id* at 203.

type of decision is common because the CIO's primary responsibility is to maximize system uptime and efficiency, a responsibility that information security often complicates.[84]

CIOs and CISOs at HHS and its operating divisions face this challenge. Several initiatives at HHS focus on the increased use of modern and advanced IT, from the PPACA-mandated FFM to the business applications developed and implemented by and for each operating division. The same conflicting goals of cost, schedule, and safety confront these initiatives just as they did the engineers and managers at NASA. The compromises at FDA, HRSA, NIH, CMS, IHS, and SAMHSA, suggest officials are responding by accepting greater risks to the security of HHS information systems in order to launch and continue operating those systems, just as their NASA counterparts did prior to both shuttle disasters. They are "normalizing deviance" within HHS's information security program.

There is no basis to believe that HHS and its operating division CIOs and CISOs are purposefully subverting the security of their own networks. However, the organizational structure currently in place at HHS and its operating divisions subordinates information security to information operations. When operational pressures mount, security is the obvious "release valve." If HHS is to address the systemic weaknesses within its information security program, then information security responsibilities must be separated from information operations responsibilities.

PART IV – RECOMMENDATIONS

HHS and each of its affected operating divisions addressed the individual vulnerabilities that led to each cyber incident detailed in this report. However, they did not implement any major policy or structural reforms to address the systemic tensions within HHS's information security program. These systemic tensions stem primarily from the inherent subordination of security to operations that the current CIO-CISO organizational structure creates. To better account for and balance these concerns, that organizational structure must be reformed.

Industry experts and analysts with whom the committee spoke described a growing trend in the private sector to restructure information security operations so that CISOs report to a senior executive other than the CIO. According to a 2014 ThreatTrack Security survey to that effect, less than half of CISOs at surveyed organizations still report to their CIO.[85] Organizations are migrating away from the traditional CIO-CISO reporting structure to eliminate the tensions between security and operations that the traditional structure creates. It also removes information security from the IT "silo" and allows experts from across the organization to see and influence information security decisions.

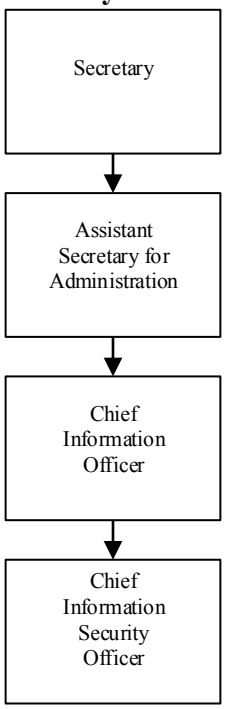
---

[84] Joe Stanganelli, *Cyber Security And The CIO: Changing The Conversation*, INFORMATIONWEEK, June 2, 2015, *available at* http://www.informationweek.com/strategic-cio/cyber-security-and-the-cio-changing-the-conversation/a/d-id/1320660.

[85] NO RESPECT: CHIEF INFORMATION SECURITY OFFICERS MISUNDERSTOOD AND UNDERAPPRECIATED BY THEIR C-LEVEL PEERS, THREATTRACK SECURITY, *available at* http://www.threattracksecurity.com/resources/white-papers/chief-information-security-officers-misunderstood.aspx.

HHS and each of its operating divisions adhere to the traditional CIO-CISO reporting structure mandated by FISMA. Figure 1 shows the current organizational structure of the offices and teams primarily responsible for information security at HHS.

Figure 1 – Current Organizational Structure of HHS/Operating Division Information Security Offices



To address the systemic weaknesses in the traditional CIO-CISO organizational structure, committee staff make the following recommendations:

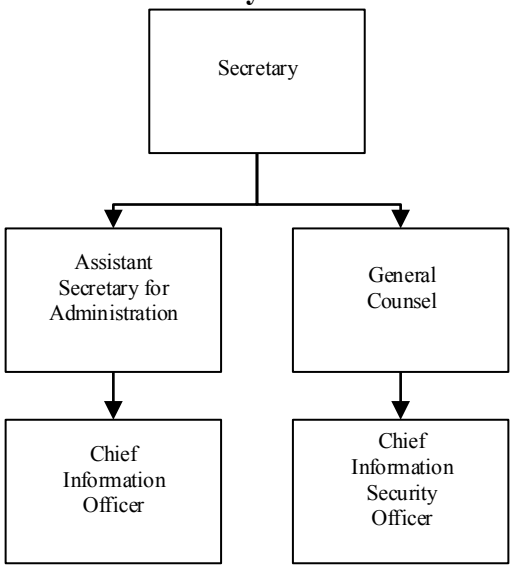
- CISOs should be designated as the primary authority responsible for information security at HHS and its operating divisions, and all information security responsibilities currently assigned to the CIO should be officially transferred to the CISO;

- The HHS Office of the CISO, including all functions, personnel, assets, and liabilities, should be removed from the Office of the CIO and relocated to the Office of the General Counsel;

- The Office of the CISO for each HHS operating division, including all functions, personnel, assets, and liabilities, should be removed from the Office of the CIO and relocated to the operating division's Office of the Chief Counsel.

This proposed reorganization is shown in Figure 2.

Figure 2 – Proposed Organizational Structure of HHS/Operating Division Information Security Offices



By seperating information security from information operations, this reorganization addresses the inherent subordination of HHS's information security program. It eliminates the ability of officials responsible for information operations to "normalize deviance" in order to ease operational pressures, as they no longer possess information security responsibilities, nor does information security exist in their chain of command. It removes information security from the IT "silo" and facilitates the inclusion of expertise across HHS in information security decisions. In particular, the placement of the CISO within the Office of the General or Chief Counsel specifically acknowledges the fact that information security has evolved into a risk-management activity, traditionally the purview of the legal team.

The compromise of an information system is no longer a purely technological issue, but one of risk and liability. Information system breaches often result in the unauthorized access of intellectual property (IP), proprietary information, or the PII of employees or customers. It is no longer enough to address and mitigate the security vulnerability or vulnerabilities that facilitated a compromise; organizations must now cope with regulations regarding the exposure of protected information, litigation, and lost business from compromised IP or reputational damage. Since the management of an organization's risk and liability is the responsibility of its legal team, it is logical to place the protection of the information systems on which an organization relies within the Office of the General or Chief Counsel. This reorganization is the first step toward creating a system that incentivizes better security.

PART V - CONCLUSION

The committee's investigation began with the October 2013 compromise at FDA, which revealed several concerns:

FDA:

(1) FDA did not take adequate actions to mitigate or prevent a well-known web vulnerability that has been a top web security concern over the last decade.

(2) FDA's security scans did not go deep enough to alert the agency that its systems were not protected against SQL injection attacks, and initially delayed FDA from realizing that there had been a breach.

(3) FDA did not encrypt PII, contrary to federal standards.

(4) FDA did not contact the inactive account holders of compromised accounts to inform them of the compromise in the immediate aftermath of the breach.

(5) FDA's failure to appoint a full-time CIO and a permanent CISO puts information security at an institutional disadvantage within FDA, as the FDA Centers leaders with permanent appointments and thus have a stronger institutional position to promote operational interests over security interests. This is illustrated by FDA restricting DHS and OIG access to certain applications during testing of FDA information security.

(6) FDA was unable to find evidence of an incident confirmed by an OIG investigation that was similar in nature to and by the same malicious actor behind an incident that another HHS operating division was able to detect in real-time.

(7) FDA was operating servers in a data center that its own security auditors would not accredit.

After committee staff learned of the additional breaches at other HHS operating divisions, additional concerns emerged:

NIH:

(1) NIH cybersecurity officials could not provide clear and consistent information about security incidents in their environment.

(2) NIH identified two separate security incidents as one incident.

SAMHSA:

(1) SAMHSA personnel identified a list of hacker aliases as a list of security vulnerabilities.

(2) SAMHSA and CSIRC originally claimed to have limited information on the incident, yet CSIRC, through an HHS legislative affairs representative, later identified the vulnerability used against SAMHSA as a XSS attack.

(3) There appears to be a compartmentalization of cybersecurity personnel at operating divisions that negatively impacts their ability to adequately protect HHS networks.

(4) HHS OIG does not share information learned from its investigations with affected operating divisions, denying those operating divisions the opportunity to incorporate "lessons learned" and improve their information security capabilities.

Department-wide:

(1) Information security at the Department does not receive adequate priority as a result of the organizational hierarchy of officials and offices.

The unsophisticated nature of the attacks used against FDA, HRSA, NIH, CMS, IHS, and SAMHSA, as well as the susceptibility of their networks to them, calls into question the adequacy of information security at HHS and its operating divisions. The committee's investigation has led committee staff to conclude that a significant weakness exists within the information security programs of these operating divisions and of HHS itself.

Evidence uncovered during the committee's investigation suggests that this weakness stems in part from the organizational structure of HHS's information security offices in which the senior official for information security is subordinated to the senior official for information operations. This structure is not designed to fairly balance the concerns of information security and information operations, which are often in conflict, and the organizational structure promotes operations over security. As a result, information security at HHS and its operating divisions is substantially weakened.

The initial investigation into the FDA breach and the additional incidents at other HHS operating divisions demonstrate the shortcomings of placing operations and security oversight within the same office. Too often, security is sacrificed for operations. The recommendations outlined in this report aim to create a system that provides a better balance of operations and security, and appropriately addresses the legal concerns arising from information security matters.