



August 2016

INFORMATION SECURITY

FDA Needs to Rectify Control Weaknesses That Place Industry and Public Health Data at Risk

GAO Highlights

Highlights of [GAO-16-513](#), a report to congressional requesters

Why GAO Did This Study

FDA has a demanding responsibility of ensuring the safety, effectiveness, and quality of food, drugs, and other consumer products. In carrying out its mission, FDA relies extensively on information technology systems to receive, process, and maintain sensitive industry and public health data, including proprietary business information such as industry drug submissions and reports of adverse reactions. Accordingly, effective information security controls are essential to ensure that the agency's systems and information are adequately protected from inadvertent or deliberate misuse, improper modification, unauthorized disclosure, or destruction.

GAO was asked to examine security controls over key FDA information systems. GAO assessed the extent to which FDA had effectively implemented information security controls to protect the confidentiality, integrity, and availability of its information on seven information systems selected for review. To do this, GAO reviewed security policies, procedures, reports, and other documents; examined the agency's network infrastructure; tested controls for the seven systems; and interviewed FDA personnel.

What GAO Recommends

GAO is making 15 recommendations to FDA to fully implement its agency-wide information security program. In a separate report with limited distribution, GAO is recommending that FDA take 166 specific actions to resolve weaknesses in information security controls. HHS stated in comments on a draft of this report that FDA concurred with GAO's recommendations and has begun implementing several of them.

View [GAO-16-513](#). For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or Dr. Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

August 2016

INFORMATION SECURITY

FDA Needs to Rectify Control Weaknesses That Place Industry and Public Health Data at Risk

What GAO Found

Although the Food and Drug Administration (FDA), an agency of the Department of Health and Human Services (HHS), has taken steps to safeguard the seven systems GAO reviewed, a significant number of security control weaknesses jeopardize the confidentiality, integrity, and availability of its information and systems. The agency did not fully or consistently implement access controls, which are intended to prevent, limit, and detect unauthorized access to computing resources. Specifically, FDA did not always (1) adequately protect the boundaries of its network, (2) consistently identify and authenticate system users, (3) limit users' access to only what was required to perform their duties, (4) encrypt sensitive data, (5) consistently audit and monitor system activity, and (6) conduct physical security reviews of its facilities. FDA conducted background investigations for personnel in sensitive positions, but weaknesses existed in other controls, such as those intended to manage the configurations of security features on and control changes to hardware and software; plan for contingencies, including systems disruptions and their recovery; and protect media such as tapes, disks, and hard drives to ensure information on them was "sanitized" and could not be retrieved after they are disposed of. The table below shows the number of GAO-identified weaknesses and associated recommendations, by control area.

Number of GAO-Identified Information Security Weaknesses at the Food and Drug Administration and Associated Recommendations, by Control Area

Control area	Number of weaknesses identified	Number of recommendations
Access controls	58	122
Configuration management	23	37
Contingency planning	5	6
Media protection	1	1
Total	87	166

Source: GAO. | GAO-16-513

These control weaknesses existed, in part, because FDA had not fully implemented an agency-wide information security program, as required under the Federal Information Security Modernization Act of 2014 and the Federal Information Security Management Act of 2002. For example, FDA did not

- ensure risk assessments for reviewed systems were comprehensive and addressed system threats,
- review or update security policies and procedures in a timely manner,
- complete system security plans for all reviewed systems or review them to ensure that the appropriate controls were selected,
- ensure that personnel with significant security responsibilities received training or that such training was effectively tracked,
- always test security controls effectively and at least annually,
- always ensure that identified security weaknesses were addressed in a timely manner, and
- fully implement procedures for responding to security incidents.

Until FDA rectifies these weaknesses, the public health and proprietary business information it maintains in these seven systems will remain at an elevated and unnecessary risk of unauthorized access, use, disclosure, alteration, and loss.

Contents

Letter		1
	Background	3
	Security Weaknesses Place Seven FDA Systems and Sensitive Data at Risk	11
	Conclusions	37
	Recommendations for Executive Action	38
	Agency Comments and Our Evaluation	39
Appendix I	Objective, Scope, and Methodology	43
Appendix II	Comments from the Department of Health and Human Services	48
Appendix III	GAO Contacts and Staff Acknowledgments	54
Tables		
	Table 1: Examples of Food and Drug Administration (FDA) Offices and Centers	7
	Table 2: Number of Access Control Weaknesses Identified at the Food and Drug Administration and Associated Recommendations	12

Abbreviations

CIO	chief information officer
CISO	chief information security officer
CVSS	Common Vulnerability Scoring System
FISMA	Federal Information Security Modernization Act of 2014 and Federal Information Security Management Act of 2002
FIPS	Federal Information Processing Standards
FDA	Food and Drug Administration
HHS	Department of Health and Human Services
ISCM	information system continuous monitoring
ISSO	Information Systems Security Officer
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
POA&M	plan of action and milestones
SMC	Systems Management Center
SP	special publication
US-CERT	United States Computer Emergency Readiness Team

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



August 30, 2016

The Honorable Fred Upton
Chairman
Committee on Energy and Commerce
House of Representatives

The Honorable Tim Murphy
Chairman
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
House of Representatives

The Honorable Joseph R. Pitts
Chairman
Subcommittee on Health
Committee on Energy and Commerce
House of Representatives

The U.S. Food and Drug Administration (FDA), an agency within the Department of Health and Human Services (HHS), is tasked with ensuring the safety, effectiveness, and quality of products that account for, according to FDA, about 20 cents of every dollar spent by Americans each year. These products include human and animal drugs, 80 percent of the food supply, biological products, medical devices, cosmetics, and radiation-emitting products. Its responsibilities include helping to speed innovations that make foods safer and medicines and medical devices safer and more effective; ensuring that the public has accurate, science-based information about medicines and devices to improve their health; regulating the manufacture, marketing, and distribution of tobacco products and reducing their use by minors; and supporting the nation's counterterrorism capability and ensuring the security of the supply of food and medical products.

In carrying out its mission, FDA relies on its information systems to conduct operations, process transactions, deliver services to constituents, and communicate with individuals and organizations. The agency collects, processes, and maintains highly sensitive information, including personally identifiable information, trade secrets, and confidential commercial information. One example of this type of information is proprietary business information used in approving drugs for market. Significant harm to FDA's reputation and economic damage to regulated

industries could result if this information is not adequately protected against cyber threats.

Given the critical role that the FDA performs and concerns over information security of federal systems, you requested that we examine security controls over key FDA systems. Our specific objective was to determine the extent to which FDA has effectively implemented information security controls to protect the confidentiality, integrity, and availability of its information on selected information systems.

To accomplish this objective, we observed and examined computer security controls over FDA's network infrastructure and systems key to FDA's mission. Specifically, we selected a non-generalizable sample of seven systems¹ for review that (1) receive, transmit, and/or process sensitive drug information; (2) are essential to FDA's mission, support its business processes, and contain or process sensitive proprietary business information; and (3) were assigned a Federal Information Processing Standard rating of moderate or high impact.² We also examined FDA's information security policies, plans, and procedures; reviewed testing of controls over key applications; interviewed agency officials; and reviewed FDA inspector general reports to identify previously reported weaknesses. More details on our scope and methodology are provided in appendix I.

We conducted this performance audit from February 2015 to August 2016 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that

¹Because we examined only 7 of the more than 80 systems FDA reported in its FISMA inventory with FIPS 199 categorizations, the results of our review of system-level controls cannot be generalized to the entire FDA environment.

²NIST, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS Publication 199 (Gaithersburg, Md.: February 2004). The standard requires agencies to categorize each information system according to the magnitude of harm or impact should the system or its information be compromised. The standard defines three impact levels where the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect (low), a serious adverse effect (moderate), or a severe or catastrophic adverse effect (high) on organizational operations, organizational assets, or individuals.

the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Information security is a critical consideration for any agency that depends on information systems and computer networks to carry out its mission and is especially important for a federal agency such as FDA, which collects, processes, and stores sensitive information on drugs and other products pending approval; the safety of food, drug, and medical products; and scientific research to inform regulatory decisions. While the use of interconnected electronic information systems allows the agency to accomplish its mission more quickly and effectively, this also exposes FDA's information to threats from sources internal and external to the agency. Internal threats can include errors, as well as fraudulent or malevolent acts by employees or contractors working within the agency. External threats include the ever-growing number of cyber-based attacks that can come from a variety of sources, including hackers, criminals, foreign nations, terrorists, and other adversarial groups.

Potential cyber attackers have a variety of techniques at their disposal, which can vastly enhance the reach and impact of their actions. For example, these attackers do not need to be physically close to their targets, their attacks can easily cross state and national borders, and they can more readily preserve their anonymity.³ Additionally, advanced persistent threats—where an adversary that possesses sophisticated levels of expertise and significant resources can use physical and cyber methods to achieve its objectives—pose increasing risks.⁴ Further, the interconnectivity among information systems presents increasing opportunities for such attacks.

This risk is highlighted by the rising number of reported security incidents at federal agencies. Specifically, the number of incidents reported by

³The objective of cyber attacks typically include an adversary establishing or extending footholds within the IT infrastructure of the targeted agency to (1) exfiltrate information; (2) undermine or impede critical aspects of a mission, program, or agency; or (3) position itself to carry out these objectives in the future.

⁴An advanced persistent threat (1) pursues its objectives repeatedly over an extended period of time, (2) adapts to defenders' efforts to resist it, and (3) maintains the level of interaction needed to achieve its objective.

federal agencies to the United States Computer Emergency Readiness Team (US-CERT) has increased dramatically in recent years.⁵ It rose from 5,503 in fiscal year 2006 to 77,183 in fiscal year 2015.

Compounding the growing number and types of threats are the deficiencies in security controls on the information systems at federal agencies. These weaknesses have resulted in vulnerabilities in systems and information and continue to place assets at risk of inadvertent or deliberate misuse; information at risk of unauthorized access, modification, or destruction; and critical operations at risk of disruption.

Accordingly, we have designated federal information security as a government-wide high-risk area since 1997, and in 2003 expanded this area to include computerized systems supporting the nation's critical infrastructure. In February 2015, we further expanded this area to include protecting the privacy of personal information that is collected, maintained, and shared by both federal and nonfederal entities.⁶ In September 2015, we reported that more than half of the 24 major federal agencies continued to experience weakness in the controls intended to preserve confidentiality—preventing unauthorized access to information and systems; integrity—preventing unauthorized modification or destruction of information, including access and configuration controls; and availability—ensuring timely and reliable access to and use of information when needed, such as contingency planning controls.⁷

⁵The Department of Homeland Security's US-CERT hosts the federal information security incident center. When incidents occur, agencies are to notify the center.

⁶See most recently GAO, *High Risk Series: An Update*, [GAO-15-290](#) (Washington, D.C.: Feb. 11, 2015).

⁷GAO, *Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs*, [GAO-15-714](#) (Washington, D.C.: Sept. 29, 2015).

To improve federal information security, the Federal Information Security Modernization Act (FISMA) was enacted in 2014.⁸ The law is intended to address the increasing sophistication of cybersecurity attacks, promote the use of automated security tools with the ability to continuously monitor and diagnose the security posture of federal agencies, and provide for improved oversight of federal agencies' information security programs. FISMA provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets.

Among other things, FISMA requires federal agencies to develop, document, and implement an agency-wide information security program. Agencies are to carry this out using a risk-based approach to information security management. Such a program includes developing and implementing cost-effective security policies, plans, and procedures; assessing risk; providing specialized training; testing and evaluating the effectiveness of controls; planning, implementing, evaluating, and documenting remedial actions to address information security deficiencies; and ensuring continuity of operations.

FISMA also gives the National Institute of Standards and Technology (NIST) responsibility for developing standards and guidelines that include minimum information security requirements. To this end, NIST has issued numerous publications to provide guidance for agencies in implementing an information security program. These include, among others, the NIST Federal Information Processing Standard (FIPS) 199,⁹ which provides requirements for agencies to categorize their systems and information, and NIST Special Publication (SP) 800-53,¹⁰ which provides guidance on

⁸The Federal Information Security Modernization Act of 2014 (FISMA 2014), Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014) partially superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers to the new requirements in FISMA 2014, FISMA 2002 requirements relevant here that were incorporated and continued in FISMA 2014 and to other relevant FISMA 2002 requirements that were unchanged by FISMA 2014 and continue in full force and effect.

⁹NIST, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS Publication 199 (Gaithersburg, Md.: February 2004).

¹⁰NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53, Revision 4 (Gaithersburg, Md.: April 2013).

the selection and implementation of information security and privacy controls for systems.

FDA Is Responsible for Ensuring the Safety, Effectiveness, and Quality of Food and Medical Products

FDA is a consumer protection agency with broad regulatory authority charged with protecting public health by ensuring the safety, effectiveness, and security of human veterinary drugs, biological products, and medical devices; ensuring the safety of foods, cosmetics, and radiation-emitting products; and regulating tobacco products.

FDA's mission includes helping to speed innovations that make foods safer and medicines and medical devices safer and more effective; ensuring members of the public have accurate, science-based information they need to use medicines, devices, and foods to improve their health; regulating the manufacture, marketing, and distribution of tobacco products and reducing tobacco use by minors; and addressing the nation's counterterrorism capability by ensuring the security of the supply of foods and medical products.

FDA performs regulatory activities that include

- reviewing and approving new drugs and certain medical products;
- inspecting manufacturing facilities for compliance with regulations and good manufacturing practices; and
- conducting post-market surveillance of food, drug, and medical products to ensure they are safe; tracking and identifying the source of outbreaks of foodborne illnesses; and issuing recall notices and safety alerts for products that threaten the public health.

According to FDA, its fiscal year 2015 appropriation was \$4.5 billion. The agency is headed by a Commissioner and is staffed by more than 14,000 employees across the United States and around the world. FDA consists of its Office of the Commissioner and four directorates that oversee the agency's core functions. These directorates are the Office of Foods and Veterinary Medicine, Office of Global Regulatory Operations and Policy, Office of Medical Products and Tobacco, and Office of Operations. Within these directorates are offices and centers that focus on core parts of the agency's mission. Examples of these offices and centers are shown in table 1.

Table 1: Examples of Food and Drug Administration (FDA) Offices and Centers

FDA Offices and Centers	Description
Office of the Commissioner	Provides centralized agency-wide program direction and management services to support FDA's mission. The office includes the National Center for Toxicological Research, which conducts peer-reviewed scientific research and provides expert technical advice and training to support FDA's science-based regulatory decisions.
Office of Foods and Veterinary Medicine	Responsible for protecting the safety and security of food for humans and animals; regulating the safety and effectiveness of animal drugs; and ensuring that food labels contain useful and reliable information. Includes the Center for Food Safety and Applied Nutrition and Center for Veterinary Medicine.
Center for Food Safety and Applied Nutrition	Helps protect the public health by ensuring that foods are properly labeled and that cosmetics are safe and properly labeled.
Center for Veterinary Medicine	Helps ensure animal food products are safe; evaluates the safety and effectiveness of drugs to treat companion and food-producing animals.
Office of Medical Products and Tobacco	Provides high-level coordination and leadership across the Centers for Biologics Evaluation and Research, Drug Evaluation and Research, Device and Radiological Health, and Tobacco Products.
Center for Biologics Evaluation and Research	Regulates and evaluates the safety and effectiveness of biological products, such as blood and blood products, vaccines and allergenic products, and protein-based drugs.
Center for Drug Evaluation and Research	Promotes and protects the public health by ensuring that prescription and over-the-counter drugs are safe; regulates drugs and reviews new drug applications.
Center for Devices and Radiological Health	Responsible for ensuring the safety and effectiveness of medical devices and preventing unnecessary human exposure to radiation from radiation-emitting products.
Center for Tobacco Products	Oversees tobacco product performance standards, reviews pre-market applications for new and modified-risk tobacco products and new warning labels, and establishes and enforces advertising and promotion restrictions.
Office of Global Regulatory Operations and Policy	Provides executive oversight, strategic leadership, and policy direction to FDA's domestic and international product quality and safety efforts, including global collaboration, global data-sharing, development and harmonization of standards, field operations, compliance, and enforcement activities. It includes the Office of Regulatory Affairs, which leads FDA field activities and provides FDA leadership on imports, inspections, and enforcement policy.
Office of Operations	Provides mission support services across the FDA and its centers, and coordinates emergency preparedness and response activities for incidents involving FDA-regulated products across FDA and its stakeholders.
Office of Information Management and Technology	Provides information technology support services across the FDA and its centers. The office is responsible for overseeing the protection of privacy and ensuring confidentiality, integrity, and availability of FDA's information in accordance with federal, department, and agency regulations.

Source: FDA. | GAO-16-513

FDA Relies on Computer Systems to Support Its Mission

FDA relies extensively on IT to fulfill its mission and support related administrative needs. Among the more than 80 systems reported in its FISMA inventory, the agency has systems dedicated to supporting its product review and evaluation activities, regulatory compliance functions, and product safety monitoring activities, as well as systems to support administrative processes. All of these systems are supported by an IT infrastructure that includes network components, critical servers, and data centers.

In fiscal year 2015, the agency reported spending \$585 million on IT, of which approximately \$12 million (or about 2 percent of the IT budget) was for information security. This percentage is lower than the approximately 8 percent of their fiscal year 2015 IT spending that the 23 civilian agencies covered by the Chief Financial Officers Act reportedly spent on information security. For fiscal year 2016, FDA requested \$640 million for IT and \$16 million for information security. In addition, FDA indicated that real-time connectivity and access to data and information is essential for its daily operations, as well as its interactions with the public and other partners. These factors depend on high-quality, high-availability, and high-performing data networks, server and application infrastructure, communications services, simple and complex computer applications, mobile workforce capabilities, and rapid and responsive service delivery.

Examples of the processing activities that key FDA systems perform in supporting of the agency's mission are listed below:

- Support and facilitate post-market product safety surveillance of human drugs, biologics, devices, and combination products. Provide a data repository for collecting, storing, viewing, analyzing, reporting, and tracking the receipt of adverse event data or medication errors.
- Establish a single gateway or communications portal for accepting electronic submissions or allowing authorized users to view or obtain information. Examples of electronic submissions include industry-provided trade secrets, adverse event records, and a multitude of different records related to FDA's regulatory oversight of regulated products.
- Provide capabilities for regulatory scientific research, while also supporting FDA's overall goals and objectives in areas where information technology requires supercomputer-strength computational power.
- Support FDA's research and development activities.

-
- Provide a platform through which FDA organizations may disseminate FDA-related information to interested parties, including the public, health professionals, regulated industries, and the media. Provide information about the various product areas that FDA regulates (food, drugs, medical devices, cosmetics, etc.), timely advisories (e.g., anticipated disease outbreaks such as the Severe Acute Respiratory Syndrome (SARS), buying medicines online, and LASIK surgery), and other FDA activities. Provide links to related reference materials and opportunities for consumers and industry to interact with the FDA.
 - Provide basic network and security capabilities for the FDA enterprise.
 - Facilitate receipt and review of electronic drug applications. This function includes scans and checks of the validity of drug submissions from industry and making them available for reviewers, as well as providing file shares for storing successful submissions that are to be reviewed.

In addition, FDA contractors support data centers and systems that provide, among other things, the network infrastructure for the agency's systems and its public website. The information handled by these systems includes sensitive or confidential business information on drug submissions and adverse event reports, among other types of information.

Accordingly, effective implementation of security controls is necessary to protecting the confidentiality, integrity, and availability of FDA's information and in preventing the occurrence or lowering the risks of security breaches similar to one the agency experienced in 2013. During that breach, an intruder gained unauthorized access to one FDA system's user accounts and passwords. Effective controls can help ensure only authorized users (people and processes) access information and systems to lessen the chances of unauthorized disclosures of information, improper changes or modifications to FDA's information and systems, and system disruptions that could hamper the agency's ability to perform its mission.

To improve the management of FDA's information systems security and operations, the agency, in fiscal year 2015, consolidated its network and security operations centers to reorganize the Systems Management Center (SMC). According to FDA, the SMC is the central command and control center and is intended to help establish real-time network awareness to forecast, detect, alert, and report events such as security incidents and facilitate the coordination requirements of its Office of Information Management and Technology. In addition, the agency

reported that it established a cybersecurity task force to address short- and long-term concerns with protecting its network boundaries.

Information Security Responsibilities at FDA

Under FISMA, the Commissioner of FDA is responsible for ensuring the confidentiality, integrity, and availability of the information and systems that support the agency and its operations. FISMA also requires that the agency head delegate to the chief information officer (CIO) the overall responsibility for management of the agency's IT security program. At FDA, the CIO is responsible for evaluating the overall mission requirements for an IT system or application and ensuring that it complies with FDA IT security policies, guidelines, and standards. The CIO is also responsible for, among other things,

- ensuring effective implementation of FDA's IT Security Policy;
- formally appointing a Chief Information Security Officer (CISO) and ensuring that individual complies with FDA's IT security regulations and guidelines;
- ensuring that IT security is included in management planning, programming budgets, and the IT capital planning process; and
- ensuring that annual security reviews are conducted to include annual review and update of security policies and reporting of IT systems to the Office of Management and Budget (OMB).

In addition, FDA's IT Security Program is headed by the agency's CISO, who is responsible for ensuring that adequate and appropriate controls are applied to FDA systems for the protection of privacy, and to ensure confidentiality, integrity, and availability, of information. The CISO is to employ security policies and standards for FDA information systems enterprise-wide in accordance with FDA, HHS, OMB, NIST, and other federal security requirements. The CISO also provides guidance on IT system security matters to the Information Systems Security Officers (ISSO) in the center/office they support.

At FDA, ISSOs are responsible for ensuring the implementation of adequate system security for each system supporting a particular center or office. Every center or office system is to have an ISSO assigned as the point of contact for security. Among other things, FDA ISSOs' responsibilities include (1) ensuring that FDA systems are operated, used, maintained, and disposed of in accordance with FDA's security policies and procedures; (2) ensuring system security plans are completed and maintained; (3) assisting with system authorization; (4)

responding to and reporting security incidents; (5) promoting security awareness; and (6) ensuring media handling procedures are followed.

Security Weaknesses Place Seven FDA Systems and Sensitive Data at Risk

FDA has taken steps to safeguard its systems that receive, process, and maintain sensitive data by, for example, implementing policies and procedures for controlling access to and securely configuring those systems. However, a significant number of weaknesses remain in technical controls—including access controls, change controls, and patch management—that jeopardize the confidentiality, integrity, and availability of its systems. An underlying reason for these weaknesses is that FDA had not yet fully implemented an agency-wide information security program to provide reasonable assurance that controls were operating effectively. These shortcomings put FDA systems at increased and unnecessary risk of unauthorized access, use, or modification that could disrupt its operations. To its credit, FDA, during the course of our work, immediately resolved some of the weaknesses identified and provided information on its proposed actions to address the underlying weaknesses in controls.

FDA Did Not Fully Implement Access Controls

Access controls are designed and implemented to provide reasonable assurance that an agency's computerized information is reliable. Both logical and physical access controls are intended to prevent, limit, and detect unauthorized access to computing resources, programs, information, and facilities. Access controls include those related to (1) protection of system boundaries, (2) identification and authentication of users, (3) authorization of access permissions, (4) encryption of sensitive information, (5) audit and monitoring of system activity, and (6) physical security of facilities.

As shown in table 2, weaknesses existed in each of these areas for the systems we reviewed. In a separate report with limited distribution, we describe these weaknesses in more detail, along with associated recommendations.

Table 2: Number of Access Control Weaknesses Identified at the Food and Drug Administration and Associated Recommendations

Access control category	Number of weaknesses	Number of recommendations
Boundary protection	7	24
Identification and authentication	13	21
Authorization	11	20
Cryptography	16	29
Audit and monitoring	10	26
Physical security	1	2
Total	58	122

Source: GAO. | GAO-16-513

Inadequate design or implementation of access controls increases the risk of unauthorized disclosure, modification, and destruction of sensitive information and disruption of service.

FDA Did Not Always Adequately Protect Its Network Boundaries

Boundary protection controls logical connectivity into and out of networks and controls connectivity to and from devices connected to the network. For example, multiple firewalls can be deployed to prevent both outsiders and trusted insiders from gaining unauthorized access to systems, and intrusion detection technologies can be deployed to defend against attacks from the Internet. Unnecessary connectivity to an organization's network increases not only the number of access paths that must be managed and the complexity of the task, but also the risk of unauthorized access in a shared environment.

NIST recommends that agencies implement subnetworks to separate publicly accessible system components from their internal networks.¹¹ NIST also states that agencies should provide adequate protection for networks and employ information control policies and enforcement mechanisms to control the flow of information between designated sources and destinations within information systems. Similarly, NIST recommends that organizations monitor and control communications at information systems' external boundaries and at key internal boundaries within a system.

¹¹NIST, Special Publication 800-53.

FDA did not always adequately ensure that its network boundaries were sufficiently segregated. For example, the contractor supporting the agency's public-facing website did not isolate the agency's network from its own network and that of its other customers, which included non-FDA customers. In addition, the contractor did not configure firewall rules to restrict access into FDA's internal network.

In another example, FDA did not sufficiently restrict inbound connections from one of its untrusted networks and isolate that network from its internal network. The network was untrusted because the agency had not developed and implemented risk management controls for the system.¹² As a result, it poses increased risks to other agency systems.

Further, as illustrated in the following examples, FDA did not always implement other boundary controls.

- Network devices at the agency's field locations were not properly configured and allowed all remote access protocols, such as the unsecure telnet protocol.
- Routers at certain international locations were not configured to restrict inbound management traffic from untrusted sites.
- Host-based firewalls for four key systems and some workstations were not effectively configured to permit only necessary traffic and provide protection from malicious activity.

As a result, sensitive public health, proprietary business, and personal information maintained by the agency were at increased risk of compromise due to inadequate separation of the service provider's network from FDA's network, inadequate separation of the untrusted network from the agency's network, and weaknesses in other boundary controls.

¹²NIST details the security risk management process as including security categorization, control selection and implementation, assessment, authorization, and continuous monitoring.

FDA Did Not Always
Implement Controls for
Identifying and Authenticating
System Users

A computer system must be able to identify and authenticate different users so that activities on the system can be linked to a specific individual. When an organization assigns a unique user account to a specific user, the system is able to distinguish that user from another—a process called identification. The system must also establish the validity of a user's claimed identity by requesting some kind of information, such as a password, that is known only by the user—a process known as authentication. The combination of identification and authentication—such as a user account/password combination—provides the basis for establishing individual accountability and for controlling access to the system.

NIST SP 800-53 recommends that password management controls should be established for information systems that include minimum password complexity requirements, password lifetime restrictions, prohibitions on password reuse, and user accounts to be temporarily locked out after a certain number of failed login attempts during a specified period of time. Further, FDA password policy outlines requirements consistent with this guidance.

NIST also states that agencies can satisfy certain identification and authentication requirements by complying with the requirements in Homeland Security Presidential Directive 12¹³ and using multifactor authentication such as personal identity verification cards.¹⁴ Multifactor authentication requires the use of two or more different factors to achieve authentication. The factors are defined as something you know (e.g., a password or a personal identification number); something you have (e.g., cryptographic identification device or token); or something you are (e.g., biometric).

¹³Homeland Security Presidential Directive 12, issued in August 2004, directed the establishment of a mandatory, government-wide standard for secure and reliable forms of identification for federal government employees and contractors that access government-controlled facilities and information systems.

¹⁴NIST defines a personal identity verification card as a physical artifact (e.g., identity card or "smart" card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, or digitized fingerprint representation) such that a claimed identity of the cardholder may be verified against the stored credentials by another person (human-readable and verifiable) or an automated process (computer-readable and verifiable).

FDA implemented personal identity verification cards for multifactor authentication; however, the agency did not always implement strong password controls in accordance with its security policies and NIST guidance on five of the seven systems we reviewed. For example, three local accounts on a database server which contained certificates used to encrypt industry partner submission packages had passwords that had not been changed in more than 5 years. In addition, several service accounts for servers with access to sensitive industry partner regulatory submissions had passwords set to never expire. Further, a Windows administrator's non-privileged account was unnecessarily elevated to a privileged account by being part of an administrators group. These accounts are used to administer users' logical access inside FDA mission-critical systems that process confidential business information or trade secrets such as that for drug submissions and adverse event reporting. In another example, the password to a service account for synchronizing user passwords was set to never expire and had not been changed in the last 6 years.

In addition, FDA did not always implement password controls on certain network devices. For example, password management settings were set to default values on two network devices that delivered web applications to FDA users. These default settings were for local accounts, including web administrator and root accounts, and included minimum password lengths set to six characters, with no requirements for password complexity, maximum password lifetime days, password history, and invalid attempts. In another example, a user account password for a network management server that monitors and maintains a history of network devices' hardware and software changes had not been changed since January 6, 2011. Without implementing strong password requirements, increased risk exists that passwords could be guessed, permitting unauthorized access to FDA systems.

FDA Users Had More Access to Information than Necessary for Official Duties

Authorization is the process of granting or denying access rights and permissions to a protected resource, such as a network, a system, an application, a function, or a file. For example, operating systems have built-in authorization features such as permissions for files and folders. Network devices, such as routers, have access control lists that can be used to authorize a user who can access and perform certain actions on the device. A key component of granting or denying access rights is the concept of "least privilege." Least privilege is a basic principle for securing computer resources and information. This principle means that a user is granted only those access rights and permissions needed to perform official duties. To improve authorization controls, the Federal CIO

instructed agencies, as part of the Cybersecurity Sprint,¹⁵ to tighten policies and practices of privileged users. These steps included, for example, minimizing the number of privileged users and limiting functions that can be performed when using privileged accounts. To avoid unintentionally authorizing user access to sensitive files and directories, an agency must give careful consideration to its assignment of rights and permissions.

NIST Special Publication 800-53 recommends that agencies should grant user accounts only those privileges required for the users to perform their job functions. Additionally, FDA policy states that access to sensitive information must be restricted and based on the concept of need-to-know.

Although FDA has developed and documented access control requirements based on least privilege and need-to-know principles, users were granted excessive permissions that were not needed for their official duties. These permissions enabled administrators and users who did not need such permissions with the authority to read, and in some cases, write and modify submissions that could contain sensitive or confidential business information on drug submissions or adverse event reporting, as illustrated below.

- Forty-nine administrators and users with access to 392 production servers had, by default, unnecessary access to file shares containing industry submissions on adverse events.
- A group account allowed 753 users unneeded access to adverse event data submissions.
- Ninety-two desktop users, via a group account, had unauthenticated access to one key system's file shares.
- 4,534 users, which included regulatory reviewers and project managers, had uncontrolled "read access" to file shares on the system that handles sensitive regulatory drug and biologic product submissions.

¹⁵In June 2015, the Federal Chief Information Officer launched the 30-day Cybersecurity Sprint, during which agencies were to take immediate actions to combat cyber threats within 30 days. Actions included patching critical vulnerabilities, tightening policies and practices for privileged users, and accelerating the implementation of multifactor or strong authentication.

According to FDA, the high number of users with access was necessary due to the high volume of regulatory submissions reviewed daily, which regularly exceeds 1,500 per day, and because staff must often access multiple sponsor submissions in order to complete their regulatory review in a timely manner.

However, for the data we reviewed, only about 2,400 users per month accessed these files, compared with the 4,534 users who were granted access. Moreover, FDA did not restrict access to privileged users groups by, for example, differentiating high-valued submission assets from low-valued ones, even though the system stored highly sensitive industry trade secret information.

In addition, for this same system, FDA allowed 39 users in the administration group and 104 users in the staff group to have read, write, and modify privileges to the submission files. The server can be accessed without a user interface and FDA does not have visibility of users' access to the submission files on the server.

As a result, FDA was at increased risk that users could inadvertently or deliberately modify these files and jeopardize the integrity of the submitted information.

FDA Did Not Always Encrypt Certain Sensitive Data

Cryptography underlies many of the mechanisms used to enforce the confidentiality and integrity of critical and sensitive information. Cryptographic tools help control access to information by making it unintelligible to unauthorized users and by protecting the integrity of transmitted or stored information. A basic element of cryptography is encryption. Encryption is the conversion of data into a form, called a cipher text, which cannot be easily understood. Encryption can be used to provide basic data confidentiality and integrity by transforming plain text into cipher text using a special value known as a key and a mathematical process known as an algorithm. NIST SP 800-53 states that agencies should use encryption to protect the confidentiality of remote access sessions and they should encrypt sessions between host systems. The

NIST standard for an encryption algorithm is Federal Information Processing Standard (FIPS) 140-2.¹⁶

FDA did not always ensure that sensitive data were effectively encrypted when transmitted or stored. For example, 59 network devices we reviewed had weak non-FIPS-compliant algorithms to encrypt user passwords. In addition, a web server supporting the receipt of industry submissions and a database server storing certificates to support secure connections for receiving submissions used non-FIPS-compliant algorithms to encrypt passwords. Furthermore, the web server's password file was encrypted by an algorithm that was outdated and had been withdrawn by NIST over 10 years ago.

As a result of using weak encryption algorithms, FDA is at increased risk that user passwords may be easier to crack and used by unauthorized individuals to gain access to systems and sensitive information.

FDA Did Not Always Audit and Monitor Activity on Its Systems

To establish individual accountability, monitor compliance with security policies, and investigate security violations, agencies need to determine what, when, and by whom specific actions have been taken on a system. Agencies can accomplish this by implementing system or security software that provides an audit trail (a log of system activity) that is used to determine the source of a transaction or attempted transaction and to monitor a user's activities. Audit and monitoring, key components of risk management, involve the regular collection, review, and analysis of auditable events for indications of inappropriate or unusual activity, and the appropriate investigation and reporting of such activity.

Audit and monitoring controls can help security professionals routinely assess computer security, perform investigations during and after an attack, and even recognize an ongoing attack. Audit and monitoring technologies include network- and host-based intrusion detection systems, audit logging, security event correlation tools, and computer forensics. NIST guidelines¹⁷ state that agencies should retain sufficient audit logs to allow monitoring of key activities, provide support for after-

¹⁶NIST, *Security Requirements for Cryptographic Modules*, FIPS 140-2 (Gaithersburg, Md.: May 2001).

¹⁷NIST, Special Publication 800-53.

the-fact investigation of security incidents, and meet agency information retention requirements.

FDA did not always implement and integrate auditing and monitoring for the seven systems we reviewed. For example, the agency did not have network monitoring visibility across its entire network. Specifically, it did not monitor IT assets used by a contractor supporting the system that provides the agency's Internet and public network. In addition, the agency did not always audit or monitor system activity on IT assets for networks supporting scientific research and high-performance computing.

The agency also did not always retain audit logs to allow monitoring of key activities and provide support for after-the-fact investigation of security incidents. To illustrate, databases supporting drug submissions and adverse event reporting did not have logging enabled for monitoring the use of special system privileges such as alter, create, and grant.

Further, FDA did not retain all records of evidence related to a 2013 security breach from an external attack on an FDA Internet application that allowed the attacker to gain access to a backend database and exfiltrate sensitive users account information. Specifically, it did not retain digital forensics data related to the attack commands and the review of dates and times of files and database entries relevant to data exfiltration of users' account data. Such information could be useful in better understanding what occurred and in preventing future occurrences.

As a result, FDA did not have information necessary for monitoring key database activities and supporting after-the-fact investigations of security incidents. In addition, the lack of evidence could prevent the agency from determining what events occurred within its systems and networks, such as lateral movements by an attacker that may occur from initial entry into a network to network discovery, hosts targeting, and data exfiltration activities to external systems.

FDA Did Not Update Physical Security Policies or Conduct Reviews of Facilities

Physical security controls restrict physical access to computer resources and protect them from intentional or unintentional loss or impairment. Adequate physical security controls over computer resources (e.g., computer facilities, network devices such as routers and firewalls, telecommunications equipment, and transmission lines) should be established that are commensurate with the risks of physical damage or access. NIST SP 800-53 recommends that agencies review and update the current physical and environmental protection policy at an organization-defined frequency and conduct an assessment of risks,

including the likelihood and magnitude of harm, to the information system and information it processes, stores, or transmits.

Consistent with federal guidance, FDA's *Information System Security and Privacy Guide* states that physical and environmental protection policies are to be reviewed and updated every 3 years. In addition, the agency's policies for its facilities state that annual physical security reviews are to be conducted. These reviews are to include, among other things, reviewing security measures in effect to compensate for any noncompliance with requirements, and corrective actions initiated or planned to eliminate deficient conditions.

While FDA developed and documented physical security policies for its facilities, they had not been reviewed and updated for about 14 years. For example, the physical security policy for its headquarters facilities was dated February 2001, and the physical security policy for field activities was dated October 2000. Neither of these policies had been reviewed and updated since they were established, even though the agency's policy requires this to occur every 3 years. In addition, the agency had not conducted required annual physical security reviews of three of its data center facilities. FDA only provided documentation to support that it had reviewed one of them, which occurred in July 2013 and was not within the annual requirement.

According to FDA's CISO and a policy analyst, gaps in reviewing and updating policies and procedures were due to personnel resource constraints and a lack of a streamlined process to review policy and procedures at the agency. As a result, FDA has diminished assurance that its computing resources are protected from inadvertent or deliberate misuse or damage.

FDA Conducted
Background
Investigations, but
Weaknesses in Other
Controls Increased Risk

In addition to access controls, other important controls should be in place to provide reasonable assurance that the confidentiality, integrity, and availability of an agency's information is protected. These controls include policies, procedures, and techniques for (1) implementing personnel security, such as background investigations, (2) managing and implementing system configurations, (3) effectively planning for system contingencies, and (4) developing and implementing procedures for disposing of media containing sensitive information. While FDA conducted background investigations according to its policy, weaknesses in other controls increased the risk of unauthorized use, disclosure, modification, or loss of the FDA's mission-sensitive information.

FDA Conducted Background Investigations for the Personnel Reviewed

The greatest harm or disruption to a system can often come from the actions, both intentional and unintentional, of individuals. These intentional and unintentional actions can be reduced through the implementation of security controls over personnel. Background checks should be done prior to an individual's authorization to access information systems, and personnel in sensitive positions should be periodically rescreened. Furthermore, FDA policy requires positions to be designated by sensitivity and risk level, and describes requirements for conducting background investigations for employees and contractors, including periodic reinvestigations of individuals in positions of higher risk or sensitivity.

FDA conducted background investigations for the employees and contractors we reviewed. Specifically, each of the 14 employees and contractors we selected had up-to-date background investigations that were consistent with the risk designation of their positions. As a result, FDA reduced its risk that it has employed or contracted for individuals with unsuitable backgrounds for accessing its systems.

FDA Did Not Always Implement Controls for Configuration Management

Configuration management is an important control that involves the identification and management of security features for all hardware and software components of an information system at a given point and systematically controls changes to that configuration during the system's life cycle. Configuration management involves, among other things, (1) verifying the correctness of the security settings in the operating systems, applications, or computing and network devices and (2) obtaining reasonable assurance that systems are configured and operating securely and as intended. In addition, establishing controls over the modification of information system components and related documentation helps to prevent unauthorized changes and ensure that only authorized systems and related program modifications are implemented. This is accomplished by instituting policies, procedures, and techniques that help make sure that all hardware, software, and firmware programs and program modifications have been properly authorized, tested, and approved.

According to NIST SP 800-53, configuration management activities should include documenting approved configuration-controlled changes to information systems, retaining and reviewing records of the changes, auditing those records, and coordinating and providing oversight for configuration change control activities through a mechanism such as a change control board. Patch management, a component of configuration management, is important for mitigating the risks associated with known

software vulnerabilities. When a software vulnerability is discovered, the software vendor may develop and distribute a patch or work-around to mitigate the vulnerability. Without the patch, an attacker can exploit the vulnerability to read, modify, or delete sensitive information; disrupt operations; or launch attacks against other systems. Outdated and unsupported software is more vulnerable to attack and exploitation because vendors may no longer provide updates, including security updates, to correct software flaws.

FDA has developed, documented, and established policies and procedures to manage configuration changes. In addition, for the systems we reviewed, FDA officials demonstrated that system changes were first requested, tracked, and approved at the system level prior to being forwarded via an automated tool to FDA's change control board as required by policy. However, FDA officials could not provide documentation to demonstrate that emergency changes to software code to remediate security vulnerabilities were tested, validated, and documented in response to the 2013 breach of its Internet-facing web application. Further, the agency did not always implement secure configuration settings for its systems. For example:

- FDA did not appropriately configure 336 devices, which could prevent proper identity enforcement of these network devices and could allow unauthorized access to other networks and devices.
- FDA used out-of-date and unsupported software on servers storing sensitive data on industry partner regulatory submissions for several of the systems we reviewed. In addition, Windows file share servers and other application servers on several systems we reviewed were out of date and had reached end-of-life, in some cases for more than 4 years past the support date.
- Two firewalls for managing contractors' access to FDA's network had operating system versions that were close to end-of-life for support, and FDA had no mitigation plans in place to manage this risk.

Similarly, FDA has developed, documented, and established a policy for managing patches that includes time frames for applying patches based on risk, and emergency and out-of-cycle patches within 48 hours of discovery. However, FDA did not always document emergency changes to software code on an application that supported its Internet services. These changes were made in response to an external Internet attack that resulted in a breach of the system's user account data.

In addition, software security updates and patches were not always installed to address known security vulnerabilities, nor were they timely. For example:

- FDA had not applied security updates and patches for network devices, switches, firewalls, specialized network devices, and servers, as well as contractor-operated network devices, in accordance with NIST's Common Vulnerability Scoring System (CVSS)¹⁸ guidelines for patching devices. CVSS prescribes that patches be installed within 30 days for critical or high-risk vulnerabilities, 60 days for moderate-risk vulnerabilities, and 90 days for low-risk vulnerabilities. FDA's policy also requires that they follow these patching time frames. However, hundreds of these devices had not been updated with the latest patches in over 3 years.
- The agency had not patched 25 servers supporting its infrastructure. For example, one sever had not been patched for 6 months, from February to August of 2015.
- FDA had not applied critical security patches to 74 of 82 host virtual servers supporting its infrastructure. In some cases these patches contained major updates to fix multiple security vulnerabilities.
- Various file share servers for three FDA systems we reviewed had not been patched since 2009.

Without proper implementation of configuration management policies and procedures and adequate security controls, FDA systems are susceptible to many known vulnerabilities.

FDA Did Not Always Plan for Contingencies

Losing the capability to process, retrieve, and protect electronically maintained information can significantly affect an agency's ability to accomplish its mission. If contingency planning is inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete information. Contingency planning consists of interim measures to recover information system services after a

¹⁸NIST Interagency Report 7435 describes the Common Vulnerability Scoring System (CVSS) as an open framework for communicating the characteristics and impacts of IT vulnerabilities. According to NIST, CVSS allows IT management to identify and assess vulnerabilities across many disparate hardware and software platforms in order to prioritize vulnerabilities and remediate those that pose the greatest risk.

disruption. Interim measures may include relocation of information systems and operations to an alternate site, recovery of information system functions using alternate equipment, or performance of information system functions using manual methods.

NIST SP 800-53 recommends that agencies establish a contingency planning policy in the event of unplanned disruptions and provide contingency training and exercises at an agency-defined frequency, among other things. In addition, NIST SP 800-34 recommends that a test plan should be designed and tested to examine applicable contingency planning elements such as notification procedures and system recovery on an alternate platform from backup media to validate the contingency capability.¹⁹ Further, FDA policy also requires functional testing of its contingency plans annually.

Consistent with NIST guidelines, FDA's *Information System Security and Privacy Guide* states that contingency planning policies are to be updated every 3 years, while information system contingency plans are to be reviewed annually. FDA's policy also requires that contingency plans be tested on an annual basis.

However, FDA did not follow its own requirements for updating and reviewing contingency policy and plans. For example, FDA's contingency planning policy was established in 2007 but was still marked as a draft document and had yet to be reviewed and updated. Further, FDA did not review, at least annually, the contingency plans for six of the seven applications and general support systems that we reviewed during fiscal year 2015 and had not developed and documented a contingency plan for the seventh system.

In addition, FDA did not adequately test five of the six contingency plans we reviewed. For example:

¹⁹NIST, *Contingency Planning Guide for Federal Information Systems*, SP 800-34 Revision 1 (Gaithersburg, Md.: May 2010). According to the guide, contingency plan testing is a critical element of a viable contingency capability. The following areas should be addressed in a contingency plan test, as applicable: notification procedures, system recovery on an alternate platform from backup media, internal and external connectivity, system performance using alternate equipment, and restoration of normal operations.

-
- For two major applications, FDA conducted procedures to mitigate system disruptions and documented those activities as tests. However, the actions performed to mitigate disruptions were not based on planned tests.
 - A planned migration was conducted for a general support system to transfer operations to a facility. However, this migration was not the result of a planned contingency test.
 - The plans for two general support systems had not been tested since 2013. However, the tests did appropriately assess elements such as notification procedures, and system recovery.

FDA staff attributed these weaknesses to the lack of a streamlined process for reviewing policies and procedures, and personnel resource constraints such as the lack of contracted staff to support FDA contingency planning and operations during an organizational transition.

By not finalizing its contingency planning policy and not annually reviewing and testing contingency plans, FDA has reduced assurance that it has implemented controls necessary for effectively continuing operations in the event of a disruption.

FDA Had Not Developed and Implemented Media Sanitization Procedures

The destruction of media and its disposal are key to ensuring the confidentiality of information. Media can include magnetic tapes, optical disks (such as compact disks), and hard drives. Agencies safeguard used media to ensure that the information they contain is appropriately controlled or disposed of. Media that is improperly disposed of can lead to the inappropriate or inadvertent disclosure of an agency's sensitive information or the personally identifiable information of its employees and customers.

NIST SP 800-53 recommends that agencies sanitize media prior to disposal and employ sanitization mechanisms to ensure information cannot be retrieved or reconstructed. FDA's policy for sanitizing computer-related storage media, including server backup tapes, states

that techniques used to sanitize media can include degaussing,²⁰ among other things.

However, FDA did not sanitize media backup tapes that were being stockpiled for disposal. Specifically, for two data center locations, media tapes were stored outside of servers and scheduled for sanitization, but had yet to be sanitized and disposed of. At one of the two data centers, we observed a number of older tapes, and FDA staff said these tapes were awaiting disposal. Specifically, staff mentioned that the legacy tapes held data from operations in prior location and were in a “holding pattern” and tentatively scheduled for decommission. Similarly, FDA staff from the second data center acknowledged that approximately 900 tapes were also awaiting disposal and that these tapes contained older servers, databases, and files resulting from a migration to updated servers tapes.

According to the data center staff, the agency had not developed, documented, and implemented a procedure for sanitizing media, but planned to have a solution by October 2016. Until FDA fully implements a process for media sanitization, the agency is at an increased risk that its sensitive information may not be adequately protected.

FDA Did Not Fully Implement Its Information Security Program, Limiting the Effectiveness of Information Security Controls

A key reason for the weaknesses in controls over FDA’s information and information systems is that it has not yet fully implemented its agency-wide information security program to ensure that controls are effectively established and maintained. If an agency does not fully implement its program, security controls may be inadequate or inconsistently applied; responsibilities may be unclear, misunderstood, or improperly implemented; and organizational and system risks may not be assessed and monitored properly. FISMA requires each agency to develop, document, and implement an information security program that, among other things, includes

- a periodic assessment of risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems;

²⁰Degaussing involves using a magnetizing field to render a hard disk or drive permanently unusable.

-
- policies and procedures that (1) are based on risk assessments, (2) cost-effectively reduce information security risks to an acceptable level, (3) ensure that information security is addressed throughout the life cycle of each system, and (4) ensure compliance with applicable requirements;
 - subordinate plans for providing adequate information security for networks, facilities, and systems or a group of information systems, as appropriate;
 - security awareness training to inform personnel of information security risks and of their responsibilities in complying with agency policies and procedures, as well as training personnel with significant security responsibilities for information security;
 - periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, and that includes testing of management, operational, and technical controls for every system identified in the agency's required inventory of major information systems;
 - a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in information security policies, procedures, or practices; and
 - procedures for detecting, reporting, and responding to security incidents.

FDA has taken steps to implement an information security program and manage information security risks for its major applications and general support systems. However, key components of its information security program have not been fully or consistently implemented.

FDA Has Taken Steps to Assess Risks, but Some Practices Have Not Been Fully Implemented.

According to NIST SP 800-30,²¹ risk is determined by identifying potential threats to the organization and vulnerabilities in its systems, determining the likelihood that a particular threat may exploit vulnerabilities, and assessing the resulting impact on the organization's mission, including the effect on sensitive and critical systems and data. Identifying and assessing information security risks are essential to determining what

²¹NIST, *Guide for Conducting Risk Assessments*, SP 800-30, Revision 1 (Gaithersburg, Md.: September 2012).

controls are required. Moreover, by increasing awareness of risks, these assessments can generate support for the policies and controls that are adopted in order to help ensure that the policies and controls operate as intended.

FDA policy requires that risk assessment results for its systems be reviewed annually, and risk assessments be updated prior to issuing a new authority to operate,²² whenever there are significant system changes, or every 3 years. FDA's assessment of risk is conducted as part of its security assessments.

Although FDA assessed risk for six of the seven systems we reviewed, it did not document the likelihood that a particular threat could exploit system vulnerabilities. For example, FDA only identified information system control weaknesses and vulnerabilities for six of the reviewed systems, but did not determine the likelihood and impact of threats to those systems. For the seventh system, FDA did not assess risk or issue a formal authority to operate. Finally, two of the six risk assessments had not been reviewed annually.

During the course of our work, FDA completed the annual review of the risk assessment for one of the two systems, and we have verified this action. However, until FDA completes comprehensive risk assessments and reviews them annually, the agency will have less assurance that it has identified the necessary controls to protect its assets.

Policies and Procedures Were Not Always Complete or Had Not Been Reviewed in a Timely Manner

A key element of an effective information security program is to develop, document, and implement risk-based policies, procedures, and technical standards that govern the security over an agency's computing environment. Information security policy is essential to establishing roles, responsibilities, and requirements necessary for implementing an information security program. The supporting procedures provide the information and guidance on implementing the policies. According to

²²NIST Special Publication 800-37 defines the authority to operate as the official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation based on the implementation of an agreed-upon set of security controls.

NIST, an agency should develop policies and procedures for each of the NIST families of security controls to facilitate the implementation of the controls.²³ Additionally, HHS and FDA policy require that policies be reviewed every 3 years to ensure that they are sufficient and consistent with federal requirements.

FDA generally took steps to develop and document policies and procedures for its information security program, but did not always document them or ensure procedures were complete. For example, while the agency has developed policies to cover 17 of 18 NIST control families, it did not develop one for system maintenance. In addition, the agency did not develop or document procedures for implementing controls in 8 of the 18 control families. The 8 control families were Audit and Accountability, Identification and Authentication, Maintenance, Media Protection, Physical and Environmental Protection, Security Planning, Systems Communication and Protection, and System Information and Integrity. Of the procedures for 10 control families that FDA provided, 3 were complete. However, procedures for 7 families were incomplete and did not include steps suggested by NIST.²⁴ For example, procedures for security awareness and training did not include procedures for covering role-based training, and those for assessment and authorization did not address continuous monitoring as recommended by NIST.²⁵

Further, FDA did not review its policies according to its own requirements. Specifically, 11 of 18 NIST-recommended policies were not reviewed within the agency-defined frequency of 3 years. For example, the agency's personnel security policy was last reviewed in 1986. Policies for

²³The first security control in each family generates requirements for specific policies and procedures that are needed for the effective implementation of the other security controls in the family. NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53, Revision 4 (Gaithersburg, Md.: April 2013).

²⁴The seven control families were Access Control, Awareness and Training, Security Assessment and Authorization, Configuration Management, Program Management, Personnel Security, and System and Services Acquisition.

²⁵According to NIST SP 800-53, role-based training is incorporated into the security awareness training control family; the assessment and authorization family covers evaluation of effective security control implementation, and continuous monitoring facilitates the ongoing awareness of threats, vulnerabilities, and information security implementation.

other controls such as those for access controls, identification and authentication, and incident response had not been reviewed in at least 7 years. FDA conducted an internal review in 2013 to identify the policies that needed to be reviewed and updated, and had established a plan of actions and milestones for updating them by November 2013. However, the agency did not meet its own deadline for reviewing and updating 11 of the 17²⁶ policies it had developed. According to FDA staff, the policies had not been reviewed and updated because the process had been too cumbersome and required a sign-off from a number of stakeholders. FDA's CISO also stated that they had been understaffed, which led to a large backlog of policies to be reviewed.

Having incomplete policies and procedures or not reviewing them reduces FDA's assurance that roles and responsibilities have been clearly assigned and understood and that personnel have the information needed to implement its policies, which could lessen the agency's ability to efficiently and effectively protect its information systems.

FDA Developed System Security Plans for Six of Seven Reviewed Systems, but They Were Incomplete and Not Annually Reviewed

FISMA requires that agencies develop and document system security plans for all major federal information systems. This requirement should be viewed as an essential part of planning adequate, cost-effective security protection for a system. According to NIST, system security plans should provide an overview of the security requirements of the system, and document and describe the security controls and security control enhancements²⁷ in place or planned for meeting those requirements. NIST also recommends that the plans be reviewed and approved by authorizing officials or designated representatives. NIST states that plans should be reviewed and updated at least annually to ensure that they continue to reflect the correct information about the system such as changes in system owners, interconnections, and authorization status,

²⁶As previously mentioned, FDA did not develop a policy for system maintenance.

²⁷Security control enhancements add functionality, specificity, or strength to base security controls; enhancements are used to provide greater protection than the base security control due to potential adverse organizational impacts or based on assessments of risk.

among other things.²⁸ Consistent with NIST, HHS and FDA policy²⁹ require FDA to review system security plans annually.

FDA created security plans and generally documented controls for six of the seven applications and general support systems we reviewed. However, the agency did not always ensure that the plans were complete, or that plans were reviewed. For example, FDA did not always fully describe the extent to which controls were implemented for each of the six system security plans we examined. Specifically, it did not document 76 of 83 NIST-required high-impact control enhancements³⁰ in the security plan for the high-impact system used in reporting adverse events. In addition, the agency did not document the control descriptions for 171 of 262 security controls and control enhancements; specifically, the description of the implementation of 171 security controls and enhancements was left blank in the plan for the system supporting FDA's infrastructure. The system has an important role in securing the agency's other systems since 68 of those systems inherit their controls from it. FDA also did not demonstrate that any of the six plans we reviewed were approved or reviewed by authorizing or senior agency officials.

According to an information system security officer, these shortfalls were related to deficiencies in their security management tool and a lack of resources. Officials stated that the tool that they used for entering information into system security plans had software flaws, which did not allow them to properly capture system security plan control descriptions; officials stated that they plan to replace the tool but could not give a firm timeline.

Until FDA develops and documents a plan for one system supporting its research and updates system security plans to reflect current federal control requirements, the agency lacks assurance that the appropriate

²⁸NIST, *Guide for Developing Security Plans for Federal Information Systems*, SP 800-18 Revision 1 (Gaithersburg, Md.: February 2006).

²⁹HHS's *Information Systems Security and Privacy Policy* and FDA's *Information System Security & Privacy Control Parameters Guide*.

³⁰According to NIST SP 800-18, system security plans should describe how the controls are implemented.

FDA Provided Security Awareness Training but Did Not Always Track and Fully Train Users with Significant Security Responsibilities

controls have been identified for the seven systems we reviewed and increases the likelihood that the controls will not be fully implemented.

According to FISMA, an agency-wide information security program must include security awareness training for agency personnel, contractors, and other users of information systems that support the agency's operations and assets. This training must cover (1) information security risks associated with users' activities and (2) users' responsibilities in complying with agency policies and procedures designed to reduce these risks. FISMA also includes requirements for training personnel who have significant responsibilities for information security. According to NIST, agencies should also document and monitor individual information system security training activities, including basic security awareness training and specialized information system security training.

Consistent with federal law and guidelines, FDA's *Information System Security and Privacy Control Parameters Guide* states that the agency should provide role-based security-related training to all personnel with significant information security responsibilities. The agency's policy also requires that employees with significant security responsibilities participate in role-based training appropriate to their security role before receiving access to the system, when required by system or role changes and every 3 years thereafter.

FDA tracked and provided security awareness training in fiscal years 2015 and 2016 to each of the 16 users we selected for review. The agency tracks its user awareness training through a vendor-provided web-based application. According to FDA, it previously provided awareness training to about 98 percent of its users during fiscal year 2015.

However, the agency did not always track role-based training for those with significant security responsibilities. For example, FDA's tracking system only identified 6 of the 16 individuals selected as having received role-based training. According to FDA personnel, the resulting list was not complete because the agency is re-engineering its process for tracking compliance of specialized security training.

In addition, it did not fully provide role-based training to those with significant security responsibilities. FDA demonstrated that 6 of the 16 individuals with significant security responsibilities we reviewed received specialized IT training. FDA responded that the remaining 10 individuals were not system administrators who required specialized training.

However, 9 of the remaining 10 individuals had significant security responsibilities, which included the deputy chief information security officer and several information systems security officers.

According to FDA staff, the agency is currently developing role-based training courses for executives and contracting officer's representatives, and will update its IT administrator module on or around October 1, 2016. Until FDA implements procedures that provide reasonable assurance that it tracks and provides role-based training to employees with significant information security responsibilities, the agency will have less assurance that staff have the adequate knowledge, skills, and abilities consistent with their roles to protect the confidentiality, integrity, and availability of the information.

FDA Did Not Fully Test Controls or Monitor Them Effectively

A key element of an information security program is to test and evaluate policies, procedures, and controls to determine whether they are effective and operating as intended. This type of oversight is a fundamental element because it demonstrates management's commitment to the security program, reminds employees of their roles and responsibilities, and identifies areas of noncompliance and ineffectiveness. FISMA requires that the frequency of tests and evaluations of management, operational, and technical controls be based on risks and occur no less than annually. OMB directs agencies to meet their FISMA-required controls testing by drawing on security control assessment results that include, but are not limited to, continuous monitoring activities. OMB also requires agencies to develop and maintain an information system continuous monitoring (ISCM) strategy and implement an ISCM program in accordance with NIST guidelines. OMB required agencies to develop their ISCM strategies by February 28, 2014.

Continuous monitoring of security controls employed within or inherited by the system is an important aspect of managing risk to information from the operation and use of information systems. The objective of continuous monitoring is to determine if the set of deployed security controls continues to be effective over time in light of the inevitable changes that occur to a system and within an agency. Such monitoring is intended to assist in maintaining an ongoing awareness of information security, vulnerabilities, and threats to support agency risk management decisions. The monitoring of security controls using automated support tools can help facilitate continuous monitoring.

FDA has taken steps to monitor security controls through bi-weekly vulnerability scanning using automated tools. The agency also conducted

annual assessments of its information systems. However, the agency did not fully or annually assess controls for 2 of the 7 systems we reviewed. To illustrate, FDA did not assess any of the security controls for a system supporting its scientific research activities. For the other system, which supports FDA's IT infrastructure, the agency had not conducted an assessment since 2013, thus not meeting FISMA's requirement to assess controls at least annually. Further, we found that FDA has not developed and documented a continuous monitoring strategy for its information systems. HHS's inspector general previously reported this weakness in fiscal years 2013 and 2014.³¹

According to FDA staff, the agency plans to assess the infrastructure system during fiscal year 2016 since the system was being restructured during fiscal year 2015. In addition, the agency plans to implement a pilot program for continuous monitoring in August 2016. Further, the agency plans to implement the Department of Homeland Security's Continuous Diagnostics and Mitigation tool in 2016 to improve continuous monitoring of its IT assets.³² Until it fully tests controls for all systems and develops and documents a continuous monitoring strategy, FDA has less assurance that controls over its information and information systems are in place and operating as intended.

Identified Security Weaknesses Were Not Always Remedied in a Timely Fashion or Based on Risk

FISMA requires that agency-wide information security programs include a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the agency. Agencies should establish procedures to reasonably ensure that all information security control weaknesses, regardless of how or by whom they are identified, are addressed through the agency's remediation processes. For each identified control weakness, the agency is to develop and implement a plan of actions and milestones (POA&M) based on findings from security

³¹U.S. Department of Health and Human Services Office of Inspector General, *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. 5, 2014) and *Review of the Food and Drug Administration's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2014*, A-18-14-30440 (Jan. 13, 2015).

³²The Department of Homeland Security Continuous Diagnostics and Mitigation program is intended to provide federal departments and agencies with a basic set of tools to support the continuous monitoring of information systems.

control assessments, security impact analyses, continuous monitoring of activities, audit reports, and other sources. When considering appropriate corrective actions to be taken, the agency should, to the extent possible, consider the potential agency-wide implications and design appropriate corrective actions to systemically address the deficiency.

FDA's *Plans of Action and Milestones Guide* is generally consistent with federal guidance, and the agency's guide specifically requires that high-risk weaknesses be corrected within 60 days.

FDA had also generally developed and documented POA&Ms for addressing security control weaknesses and made efforts to consider agency-wide implications of security weaknesses. However, it did not always complete remedial actions in a timely manner in accordance with the agency's established deadlines or risk requirements. To illustrate, for the seven major applications and general support systems we examined, 183 of 611 (roughly 30 percent) of the POA&Ms had not been remedied by their scheduled completion date, 30 of which were identified as high risk and not corrected within the agency-defined requirement of 60 days. Of the 183 delayed POA&Ms, 102 had a scheduled completion date of 2013 or earlier. As a further example, FDA's remedial action plans listed two high-risk weaknesses identified by its Office of Inspector General in 2006 and 2007, but FDA had not mitigated these weaknesses even though the agency had planned completion dates in 2012.

FDA personnel stated that they faced challenges in remediating POA&Ms in a timely manner and based on risk. According to FDA personnel, there was a large volume of open POA&Ms and insufficient resources, which delayed addressing weaknesses in a timely manner: as of the first quarter of 2015, FDA had 1,265 open POA&Ms. FDA staff also noted that risk is considered in prioritizing remediation, but that other factors such as available resources and business impacts are also considered. FDA personnel stated that, because of the large number of open POA&Ms, they will go after "low-hanging fruit," favoring remediation of a larger number of POA&Ms over concentrating on high-risk weaknesses.

By not resolving identified weaknesses in a timely manner, or in accordance with its own policy, FDA faces an increased likelihood that weaknesses, including high-risk vulnerabilities, will go uncorrected, be exploited, and result in greater harm to agency systems and information.

FDA Did Not Fully Implement
Elements of Its Incident
Response Program

Even with strong information security controls, incidents can still occur. Agencies can reduce the risks associated with these events by detecting and promptly responding before significant damage is done. A key element of an effective incident response program includes implementing comprehensive policies, procedures, and controls in order to rapidly detect incidents, minimize loss and destruction, mitigate the weaknesses that were exploited, and restore computing services. NIST SP 800-53 recommends that agencies review and update their incident response policy and procedures at an organization-defined frequency. NIST also recommends that an organization coordinate its incident handling activities with contingency planning activities so that during a severe incident, the agency has actions in place to keep its business operational. NIST further recommends that agencies implement lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly.

While FDA has developed and documented an incident response policy, the agency did not comply with its own policy of updating its incident response policy every 3 years. The policy has not been updated since it was created in January 2007.

Further, neither FDA's incident response policy nor its procedures require or describe steps for coordinating incident response activities with planning for contingencies or system disruptions. The agency also did not update its incident response procedures using the results of lessons learned from prior incident response table top exercises we examined. For example, results from a 2012 table top exercise indicated that FDA should better train its employees so that newer, less-experienced staff are better able to respond to significant cyber incidents, and that FDA should update its procedures to include training requirements. However, the lessons learned were not incorporated into FDA's incident response procedures. Without effective incident response practices in place, FDA has reduced assurance that its systems and information are protected and that it can respond to incidents.

In response to our findings, FDA staff mentioned that the agency is in the process of incorporating lessons learned from incident handling activities into its incident response procedures, training, and testing. In addition, the agency stated that it is taking various steps to address incident response

based on our feedback from previous surveys and data requests. The agency stated that it has discontinued its incident response standard operating procedure and was developing a new one based on NIST SP 800-61.³³ The agency's staff also mentioned that personnel will undergo security training and that FDA is piloting various products to improve the agency's overall security posture, including incident response. We have not yet verified that the agency has implemented these actions, but such actions could improve FDA's incident response capability.

Conclusions

Although FDA has implemented numerous controls and taken steps intended to protect its information and information systems, pervasive control weaknesses continue to jeopardize the confidentiality, integrity, and availability of its sensitive information. In fiscal year 2015, the agency centralized the management and location of its network and security operations with intended goals that include establishing real-time network awareness and improved incident detection. The agency also immediately resolved some of the weaknesses we identified during this review. Nonetheless, significant weaknesses in controls for preventing or limiting unauthorized access to its systems and information, as well as weaknesses in other controls, such as those for ensuring that software and hardware are updated and securely configured and that sensitive media is disposed of, put FDA's systems at risk. This is significant considering that these systems handle proprietary business data from companies in multiple industries and sensitive public health data.

An underlying cause for many of these weaknesses is that FDA has not fully implemented its agency-wide information security program, such as developing and documenting appropriate policies and procedures, ensuring security controls are tested effectively, remediating weaknesses in a timely manner, and planning for contingencies or system disruptions and effectively managing risks. The widespread weaknesses in technical controls and the incomplete implementation of program elements suggest that the agency has not made effective information security a high enough priority. Until FDA implements these practices and controls, it will have limited assurance that its information and information systems are

³³NIST, *Computer Security Incident Handling Guide*, SP 800-61, Revision 2 (Gaithersburg, Md.: August 2012).

adequately protected against unauthorized access, disclosure, modification, or loss.

Recommendations for Executive Action

To effectively implement key elements of the Food and Drug Administration's (FDA) information security program, we are recommending that the Secretary of Health and Human Services direct the Commissioner of FDA to implement the following 15 recommendations:

1. Complete a risk assessment and authorization to operate for one FDA system.
2. Ensure that completed risk assessments for six systems reviewed address the likelihood and impact of threats to FDA.
3. Develop a policy for system maintenance.
4. Develop procedures for the following 8 security control families: Audit and Accountability, Identification and Authentication, Maintenance, Media Protection, Physical and Environmental Protection, Security Planning, Systems Communication and Protection, and System Information and Integrity.
5. Enhance procedures for the following 7 security control families: Access Control, Awareness and Training, Security Assessment and Authorization, Configuration Management, Program Management, Personnel Security, and System and Services Acquisition.
6. Review and update as needed per FDA's frequency, the policies for the following 11 security control families: Access Control, Audit and Accountability, Contingency Planning, Identification and Authentication, Incident Response, Media Protection, Physical and Environmental Protection, Security Planning, Personnel Security, System and Services Acquisition, and System and Information Integrity.
7. Develop and document a security plan for one system supporting FDA's scientific research.
8. Update security plans to ensure the plans fully and accurately document the controls selected and intended for protecting each of the six systems.
9. Review and approve security plans for the six systems reviewed at least annually.

-
10. Implement a process to effectively monitor and track training for personnel with significant security roles and responsibilities.
 11. Ensure that personnel with significant security responsibilities receive role-based training.
 12. Test controls at least annually for the two systems that support FDA's scientific research and IT infrastructure.
 13. Implement remedial actions in accordance with FDA's prescribed time frames or update milestones if actions are delayed.
 14. Update FDA's incident response policy in accordance with agency requirements.
 15. Update incident response procedures to include (1) instructions for coordinating incident response with contingency planning and (2) lessons learned from incident response tests.

We are also making 166 technical recommendations in a separate report with limited distribution. These recommendations address information security weaknesses related to boundary protection, identification and authentication, authorization, cryptography, physical security, configuration management, and media protection.

Agency Comments and Our Evaluation

We received written comments on a draft of this report from the Department of Health and Human Services (HHS). In the comments (reprinted in appendix II), the department stated that FDA concurred with our recommendations, has begun implementing several of them, and is actively working to address all the recommendations as quickly and completely as possible. The department also stated that FDA has acquired third-party expertise to assist in these efforts to immediately address the recommendations in our report.

The department emphasized its commitment to protecting the public health and proprietary business information at FDA, including by implementing layered defenses and other compensating controls. HHS further noted that FDA has not experienced a major cybersecurity-related breach that exposed industry or public health information and that information security remains a high priority at FDA. The department added that since hiring its CIO in 2015, FDA has undertaken steps to better ensure the prevention, detection, and correction of incidents. These include the development of an IT strategic plan and the restructuring of cybersecurity leadership, among other initiatives.

In addition, HHS noted that we did not identify an elevated risk of exposure and/or exfiltration of trade secret and/or other sensitive information. However, this does not accurately reflect the results of our review. As stated in the report, we identified a significant number of weaknesses in technical controls—including access controls, change controls, and patch management—that jeopardize the confidentiality, integrity, and availability of the seven moderate- and high-impact systems we reviewed. Moreover, several of these weaknesses affected FDA's general support systems, which are connected to numerous systems beyond the ones we reviewed. As previously mentioned, these weaknesses place the seven FDA systems, including those that receive, process, and maintain sensitive industry and public health data, at increased and unnecessary risk of unauthorized access, use, or modification.

The department also made additional comments regarding our report and methodology. In particular, it stated that our methodology did not use an industry-standard approach to assessing risk, defined as the likelihood of a given threat source exploiting a particular vulnerability and the resulting significance of the impact of that adverse event on the organization, or quantify this risk in our overall assessment. We did not perform a comprehensive risk assessment of FDA's information systems and information because that is FDA's responsibility, not ours. However, we did consider the elements of risk to agency systems and information during our review. For example, as stated in the report, in selecting the seven systems we reviewed, we considered FDA's categorization of the impact or magnitude of harm to the agency's operations, assets, and individuals should the confidentiality, integrity, or availability of the systems and the information they contain be compromised. Six of the seven³⁴ systems we selected were assigned a Federal Information Processing Standard rating of moderate or high impact by FDA, indicating that the loss of confidentiality, integrity, or availability of these systems or the information they contain would have either a serious or severe/catastrophic impact on the organization. We also considered how each control weakness, vulnerability, or program shortcoming we identified could impair or diminish the effectiveness of a security control or be exploited to facilitate unauthorized system activity. Our report identifies

³⁴FDA did not assign a Federal Information Processing standard rating for one system.

numerous weaknesses and vulnerabilities along with their potential impact if the vulnerabilities are exploited. It is also noteworthy that our work determined that for the reviewed systems, FDA had not determined the likelihood and impact of threats to those systems.

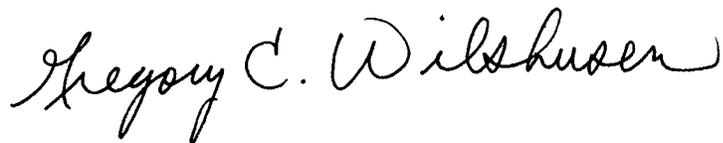
HHS also stated that our report did not consider other FDA tools, resources, and capabilities designed to prevent, detect, and correct incidents, such as its ability to prevent or mitigate breaches like the one that occurred in October 2013. We recognize that FDA has implemented numerous security controls and key elements of its information security program; however, the weaknesses we identified nevertheless pose increased and unnecessary risk to its systems and information. For example, as noted in our report, FDA had not updated its incident response policy since 2007 or incorporated other key elements. Having a complete and up-to-date incident response capability is essential to ensuring that FDA staff have the knowledge and tools to effectively respond to security incidents, such as breaches.

Finally, the department stated that our report does not consistently or clearly distinguish which of the systems reviewed contained sensitive information and which do not. It noted, for example, that FDA's Scientific Network is a research and development network that does not contain trade secret information. However, as we noted in our report, FDA's systems operate in an interconnected and networked environment, and the agency had not ensured that the Scientific Network, for example, was adequately isolated from other systems containing sensitive data, nor had it developed and implemented risk management controls for this system. These weaknesses could provide an attacker with a pathway from this less-secure system to other systems containing sensitive public health or proprietary business data. Such weaknesses therefore pose an increased risk to the sensitive information FDA collects and maintains.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to relevant congressional committees, the Secretary of Health and Human Services, the Commissioner of FDA, and other interested parties. In addition, the report will be available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions about this report please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or Dr. Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov. Contact

points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix III.



Gregory C. Wilshusen
Director, Information Security Issues



Dr. Nabajyoti Barkakati
Director, Center for Technology and Engineering

Appendix I: Objective, Scope, and Methodology

The objective of our review was to evaluate the extent to which the Food and Drug Administration (FDA) has implemented information security controls to effectively protect the confidentiality, integrity, and availability of its information on selected information systems.

To determine the effectiveness of the FDA's security controls, we gained an understanding of the overall network environment, identified interconnectivity and control points, and examined controls for the agency's networks and facilities. We reviewed controls over the network infrastructure and selected systems that processed confidential commercial and proprietary business information. We performed our work at FDA headquarters in Silver Spring, Maryland, and at several data centers in Ashburn, Virginia, and Silver Spring, Maryland.

We selected a non-generalizable sample of seven systems¹ for review that (1) receive, transmit, and/or process sensitive drug information; (2) are essential to FDA's mission, support its business processes, and contain or process sensitive proprietary business information; and (3) were assigned a Federal Information Processing Standard rating of moderate or high impact.² These systems perform the following support functions:

- Support and facilitate post-market product safety surveillance of human drugs, biologics, devices, and combination products. Provide a data repository for collecting, storing, viewing, analyzing, reporting, and tracking the receipt of adverse event data or medication errors.
- Establish a single gateway or communications portal for accepting electronic submissions or allowing authorized users to view or obtain information. Examples of electronic submissions include industry-

¹Because we examined only 7 of the more than 80 systems FDA reported in its FISMA inventory with FIPS 199 categorizations, the results of our review of system-level controls cannot be generalized to the entire FDA environment.

²NIST, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS Publication 199 (Gaithersburg, Md.: February 2004). The standard requires agencies to categorize each information system according to the magnitude of harm or impact should the system or its information be compromised. The standard defines three impact levels where the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect (low), a serious adverse effect (moderate), or a severe or catastrophic adverse effect (high) on organizational operations, organizational assets, or individuals.

provided trade secrets, adverse event records, and a multitude of different records related to FDA's regulatory oversight of regulated products.

- Provide capabilities for regulatory scientific research, while also supporting FDA's overall goals and objectives in areas where information technology requires supercomputer-strength computational power.
- Support FDA's research and development activities.
- Provide a platform through which FDA organizations may disseminate FDA-related information to interested parties, including the public, health professionals, regulated industries, and the media. Provide information about the various product areas that FDA regulates (food, drugs, medical devices, cosmetics, etc.), timely advisories (e.g., anticipated disease outbreaks such as the Severe Acute Respiratory Syndrome (SARS), buying medicines online, and LASIK surgery), and other FDA activities. Provide links to related reference materials and opportunities for consumers and industry to interact with the FDA.
- Provide basic network and security capabilities for the FDA enterprise.
- Facilitate receipt and review of electronic drug applications, to include scans and checks of the validity of drug submissions from industry and making them available for reviewers, as well as providing file shares for storing successful submissions that are to be reviewed

To evaluate FDA's controls over its information systems, we used our *Federal Information System Controls Audit Manual*,³ which contains guidance for reviewing information system controls that affect the confidentiality, integrity, and availability of computerized information; National Institute of Standards and Technology (NIST) standards and guidelines; Department of Health and Human Services guidelines; FDA policies and procedures; and standards and guidelines from relevant security and IT security organizations, such as the National Security Agency and the Center for Internet Security, and the Interagency Security Committee.

³GAO, *Federal Information System Controls Audit Manual (FISCAM)*, [GAO-09-232G](#) (Washington, D.C.: February 2009).

Specifically, we

- reviewed firewall configurations, among other things, to determine whether system boundaries had been adequately protected;
- reviewed the complexity and expiration of password settings to determine if password management was being enforced;
- analyzed administrative users' system access permissions to determine whether their authorizations exceeded that necessary to perform their assigned duties;
- observed configurations for providing secure data transmissions across the network to determine whether sensitive data were being encrypted;
- reviewed software security settings to determine if modifications of sensitive or critical system resources had been monitored and logged;
- observed physical access controls to determine if computer facilities and resources were being protected from espionage, sabotage, damage, and theft;
- examined configuration settings and access controls for routers, network management servers, switches, and firewalls;
- inspected key servers and workstations to determine if critical patches had been installed and/or were up-to-date;
- examined contingency plans for seven systems to determine whether those plans had been developed and tested;
- reviewed media handling procedures to determine if equipment used for clearing sensitive data had been tested to ensure correct performance; and
- reviewed personnel clearance procedures to determine whether staff had been properly cleared prior to gaining access to sensitive information or information systems.

Using the requirements identified by the Federal Information Security Modernization Act of 2014 (FISMA),⁴ which establishes key elements for an effective agency-wide information security program, and associated NIST guidelines, Department of Health and Human Services and Food and Drug Administration Requirements, we evaluated FDA's information security program by

- reviewing assessments of risk for six⁵ FDA systems to determine whether threats and vulnerabilities were being identified;
- analyzing FDA policies, procedures, and practices to determine their effectiveness in providing guidance to personnel responsible for securing information and information systems;
- analyzing security plans for six⁶ systems to determine if those plans had been documented and updated according to federal guidance;
- examining the security awareness training for employees and contractors to determine whether they had received training according to federal requirements;
- examining training records for personnel who have significant responsibilities to determine whether they had received training commensurate with those responsibilities;
- analyzing FDA's procedures and results for testing and evaluating security controls to determine whether management, operational, and technical controls for seven systems had been sufficiently tested at least annually and based on risk;

⁴The Federal Information Security Modernization Act of 2014 (FISMA 2014), Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014) partially superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers to the new requirements in FISMA 2014, FISMA 2002 requirements relevant here that were incorporated and continued in FISMA 2014 and to other relevant FISMA 2002 requirements that were unchanged by FISMA 2014 and continue in full force and effect.

⁵FDA did not establish a risk management process for one system, so no supporting documentation was available to review. NIST Special Publication 800-37 details the security risk management process as including security categorization, control selection and implementation, assessment, authorization, and continuous monitoring.

⁶See footnote 5.

- reviewing FDA's implementation of continuous monitoring practices to determine whether the agency had developed and implemented an information system continuous monitoring strategy to manage its IT assets and monitor the security configurations and vulnerabilities for those assets;
- examining FDA's process to correct weaknesses and to determine whether remedial action plans complied with federal guidance; and
- reviewing FDA's implementation of incident response practices.

To determine the reliability of FDA's computer-processed data, we evaluated the materiality of the data to our audit objective and assessed the data by various means, including reviewing related documents, interviewing knowledgeable agency officials, and reviewing internal controls. Through a combination of methods, we concluded that the data were sufficiently reliable for the purposes of our work.

We conducted this performance audit from February 2015 to August 2016 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Appendix II: Comments from the Department of Health and Human Services



DEPARTMENT OF HEALTH & HUMAN SERVICES

OFFICE OF THE SECRETARY

Assistant Secretary for Legislation
Washington, DC 20201

JUN 21 2016

Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. Wilshusen:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, "*Information Security: FDA Needs to Address Control Weakness that Place Industry and Public Health Data at Risk*" (GAO-16-513).

The Department appreciates the opportunity to review this report prior to publication.

Sincerely,

A handwritten signature in cursive script that reads "Jim R. Esquea".

Jim R. Esquea
Assistant Secretary for Legislation

Attachment

GENERAL COMMENTS OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED: INFORMATION SECURITY: FDA NEEDS TO RECTIFY CONTROL WEAKNESSES THAT PLACE INDUSTRY AND PUBLIC HEALTH DATA AT RISK (GAO-16-513)

The U.S. Department of Health and Human Services appreciates the opportunity to review and comment on this report.

The FDA has already begun implementing several of GAO's recommendations, and is actively working to address all recommendations as quickly and as completely as possible. In support of this effort, the FDA has acquired industry-leading expertise, Deloitte, to assist in the development and execution of timely action plans, as well as program/project management activities to immediately address the recommendations outlined in the report.

We are committed to protecting the public health and business proprietary information at the FDA, including by implementing layered defenses and other compensating controls. To date, GAO has not identified—and FDA is not aware of—an elevated risk of exposure and/or exfiltration of trade secret and/or other sensitive information.

The FDA has not experienced a major cybersecurity-related breach that exposed industry or public health information. Information security remains a high priority at the FDA, and we do not take lightly our responsibility for protecting industry and public health information. The agency recognizes the risks associated with operating this large global IT enterprise and has implemented processes, procedures, and tools to better ensure the prevention, detection and correction of incidents. This transformation began with the hiring of the FDA's Chief Information Officer (CIO) in May 2015. As an immediate first step, the CIO developed the IT Strategic Plan, which was published in October 2015. The strategic plan included many of the issues that were highlighted in the report (e.g., outdated policies). Furthermore, under the new CIO, the leadership of Cybersecurity was restructured and various initiatives were started, prior to the completion of this study, within our cybersecurity program. These activities and initiatives were initiated to ensure our IT systems and sensitive information is appropriately protected by safeguarding against unauthorized disclosure, access, or misuse and include:

- Identified information protection as our Cybersecurity Program top strategic priority.
- Monitoring inbound/outbound FDA internet traffic for anomalies by DHS Trusted Internet Connection (TIC), HHS Computer Security Incident Response Center (CSIRC), and the FDA Systems Management Center (SMC).
- Implemented and activated the FDA Systems Management Center (SMC) to unify Network and Security Operations Centers to monitor systems and conduct cybersecurity threat management activities. The SMC is the central command and control center that provides real-time network awareness to forecast, detect, alert, and report events, such as security incidents.
- Implemented the High Value Asset/Crown Jewels Initiative to provide 24x7 monitoring of the FDA critical systems (i.e. Electronic Submission Gateway (ESG), Electronic Document Room (EDR)).
- Acquired industry leading expertise (Deloitte) to provide support and advisory internal control services necessary to develop action plans to immediately address the GAO audit findings, 87 weaknesses and 166 technical recommendations. The outside firm will also

provide execution support and program/project management activities to implement the 15 GAO report recommendations for improving the Cybersecurity program.

- Immediately addressed the most concerning weaknesses identified in the Scientific Network environment in early February 2016.
- Updated our incident response procedures and enhanced our advance forensics and insider threat capabilities.
- Coordinating the implementation of Data Loss prevention and Multi-factor authentication tools and capabilities.
- Reduced our plan of actions and milestones (POA&Ms) by 31% since the arrival of the CIO (within the past year). A Plan of Action and Milestones (POA&M) is mandated by the Federal Information Systems Management Act of 2002 (FISMA) and OMB as a corrective action plan for tracking and planning the resolution of information security weaknesses.
- Established the Scientific Computing Cybersecurity Task Force to strengthen and protect the FDA's scientific and research computing capabilities and infrastructure to meet business needs.
- Aligned the counterintelligence, advanced forensics, insider threat, and other law enforcement investigations, and national security related activities under the FDA Chief Information Security Officer to address immediate cybersecurity threats, vulnerabilities and risks.
- Enhanced information sharing by activating Homeland Security Data Network (HSDN) to support CSIRT operations, intelligence, cybersecurity, and insider threat activities.
- Implemented Cybersecurity Dashboard Monthly Performance Metrics Reporting process to collect, analyze and report information regarding the performance of cybersecurity activities.
- Ramping up our IT Security budget and making appropriate investments to ensure the IT infrastructure changes and security improvements are made.

Although FDA is working to implement GAO's recommendations, FDA has several comments regarding GAO's report and methodology. First, FDA notes that risk is defined by industry and in the Federal Information System Controls Audit Manual (FISCAM) as a function of the likelihood (low, moderate or high) of a given threat-source exploiting a particular potential vulnerability, and the resulting significance of the impact of that adverse event on the organization. This industry-standard approach to assessing risk was not used in the GAO's methodology nor quantified in its overall assessment. Second, the commentary contained within the report does not consider other FDA tools, resources, and capabilities designed to prevent, detect and correct incidents. For example, the report highlights an October 2013 security incident that happened during the government shutdown. Despite having limited staff due to the shutdown, FDA cybersecurity analysts were able to mitigate the breach to limit and minimize the exposure within a matter of hours, demonstrating that the detection and correction aspects of our cybersecurity program are strong and function appropriately when needed. FDA cybersecurity tools, capabilities, and personnel prevent millions of potential attacks on a monthly basis. In fact, in February alone, we thwarted 1.16 billion attempts to penetrate our system. Third, the report does not consistently or clearly distinguish which of the audited systems contained sensitive information and which did not. For example, the scientific network is a research and development network that does not contain trade secret information.

Recommendation 1. Complete a risk assessment and authorization to operate for one FDA system.

FDA concurs with this recommendation and will complete a formal risk assessment and authorization to operate for a specific system noted in the report. The assessment will be conducted in accordance with OMB (Circular A-130), HHS and FDA policies, and other federal requirements as applicable. In addition, the FDA has taken immediate action to remediate this issue, including the completion of a preliminary risk assessment, implementation of additional technical safeguards, and the establishment of a task force that will have formalized oversight of the system associated with this GAO recommendation.

Recommendation 2. Ensure that completed risk assessments for six systems reviewed address the likelihood and impact of threats to the FDA.

FDA concurs with this recommendation and will implement process enhancements to ensure that risk assessments for the six systems reviewed by the GAO include an evaluation of the likelihood and impact of threats to the FDA.

Recommendation 3. Develop a policy for system maintenance.

FDA concurs with this recommendation and will develop a Staff Manual Guide (i.e., policy(s)) to address system and network maintenance. The Staff Manual Guide will address roles, responsibilities, management commitment, coordination among FDA stakeholders and compliance mandates.

Recommendation 4. Develop procedures for the following eight security control families: Audit and Accountability, Identification and Authentication, Maintenance, Media Protection, Physical and Environmental Protection, Security Planning, Systems Communication and Protection, and System Information and Integrity.

FDA concurs with this recommendation and has partnered with an industry leader in cybersecurity consulting, Deloitte, to develop action plans and support program/project management activities associated with this recommendation.

Recommendation 5. Enhance procedures for the following seven security control families: Access Control, Awareness and Training, Security Assessment and Authorization, Configuration Management, Program Management, Personnel Security, and System and Services Acquisition.

FDA concurs with this recommendation and agrees that procedural enhancements will further strengthen the FDA's ability to protect information and minimize risk. The FDA will assess and enhance procedures for the seven security control families identified by the GAO.

Recommendation 6. Review and update as needed per FDA's frequency, the policies for the following 11 security control families: Access Control, Audit and Accountability, Contingency Planning, Identification and Authentication, Incident Response, Media Protection, Physical and Environmental Protection, Security Planning, Personnel Security, System and Services Acquisition, and System and Information Integrity.

FDA concurs with this recommendation and has already begun revising the policies identified by the GAO and has already made significant progress. Specifically, the FDA has finalized or drafted robust information security policies addressing Access Control, Contingency Planning, and Audit and Accountability.

Recommendation 7. Develop a security plan for one system.

FDA concurs with this recommendation and will develop a security plan for the system identified by the GAO, which will align with NIST Special Publication 800-18, "Guide for Developing Security Plans for Federal Information Systems." The plan will provide an overview of the system security requirements to meet control objectives identified within NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations." The FDA will develop this plan with input from FDA management that oversees the system, including information owners, the system owner, and the information system security officers.

Recommendation 8. Update security plans to ensure the plans fully and accurately document the controls selected and intended for protecting each of the six systems.

FDA concurs with this recommendation and will update the security plans associated with each of the six systems reviewed by the GAO. These plans will be revised in alignment with NIST Special Publication 800-18 to fully and accurately document controls selected for protecting each of the six systems.

Recommendation 9. Review and approve security plans for the six systems reviewed at least annually.

FDA concurs with this recommendation and will enhance its risk management processes to include a formalized review and approval process for security plans for each of the six systems reviewed by the GAO. These reviews will occur annually, at a minimum, or more frequently if changes occur.

Recommendation 10. Implement a process to effectively monitor and track training for personnel with significant security roles and responsibilities.

FDA concurs with this recommendation and will implement a formal process in accordance with National and Departmental standards to monitor and track training requirements for personnel with significant security roles and responsibilities.

Recommendation 11. Ensure that personnel with significant security responsibilities receive role-based training.

FDA concurs with this recommendation and is developing role-based training for executives, contracting officer's representatives, and privileged users. This training will be provided to all FDA personnel whose job functions require specialized knowledge in information security.

Recommendation 12. Test controls for two systems at least annually.

FDA concurs with this recommendation and will test controls on an annual basis for the two systems identified by the GAO. Control assessments will be conducted in accordance with OMB (Circular A-130), NIST (Special Publication 800-53A), and FDA policies.

Recommendation 13. Implement remedial actions in accordance with FDA's prescribed time frames or update milestones if actions are delayed.

FDA concurs with this recommendation and has been working to enhance existing procedures and will allocate additional resources to improve POA&M management. A Plan of Action and Milestones (POA&M) is mandated by the Federal Information Systems Management Act of 2002 (FISMA) and OMB as a corrective action plan for tracking and planning the resolution of information security weaknesses. The FDA has partnered with a global leader in cybersecurity consulting, Deloitte, to address this issue.

Recommendation 14. Update FDA's incident response policy in accordance with agency requirements.

FDA concurs with this recommendation and is currently revising its incident response policy to meet agency requirements. This revised policy will align with NIST Special Publication 800-61.

Recommendation 15. Update incident response procedures to include (1) instructions for coordinating incident response with contingency planning and (2) lessons learned from incident response tests.

FDA concurs with this recommendation and will revise its current incident response procedures to include the GAO's recommendations.

Agency leadership remains committed to fostering greater information security at the FDA, and looks forward to addressing and building upon all of the above recommendations.

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

Gregory C. Wilshusen, (202) 512-6244 or wilshuseng@gao.gov
Dr. Nabajyoti Barkakati, (202) 512-4499 or barkakatin@gao.gov

Staff Acknowledgments

In addition to the individuals named above, Gary Austin, West Coile, Larry Crosland, and Chris Warweg (Assistant Directors); Vernetta Marquis (Analyst in Charge); Alexander Anderegg, Angela Bell, Saar Dagani, Angel Ip, Lee McCracken, Constantine Papanastasiou, Dwayne Staten, and Michael Stevens made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (<http://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <http://www.gao.gov> and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).
Subscribe to our [RSS Feeds](#) or [E-mail Updates](#).
Listen to our [Podcasts](#) and read [The Watchblog](#).
Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <http://www.gao.gov/fraudnet/fraudnet.htm>

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548



Please Print on Recycled Paper.