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.