GAO@100

Highlights

Highlights of GAO-22-104467, a report to congressional requesters

December 2021

CYBERSECURITY

NIH Needs to Take Further Actions to Resolve Control Deficiencies and Improve Its Program

Why GAO Did This Study

NIH responsibilities include conducting research on the prevention of infectious diseases such as COVID-19, administering over $30 billion annually in medical research grants, and supporting research on pathogens, including those that have the potential to pose a severe threat to public health and safety. In carrying out its mission, NIH relies extensively on information technology systems to receive, process, and maintain sensitive data. Accordingly, effective information security controls are essential to ensure the confidentiality, integrity, and availability of the agency's systems.

GAO was asked to examine cybersecurity at NIH. In June 2021, GAO issued a limited official use only report on the extent to which NIH had effectively implemented system controls and an information security program to protect the confidentiality, integrity, and availability of its information on selected information systems.

This current report is a public version of the June 2021 report based on GAO's review of the agency's information security program and 11 selected systems. In addition, for this public report, GAO determined the extent to which NIH has taken corrective actions to address the previously identified security program and system control deficiencies and related recommendations for improvement. GAO reviewed supporting documents regarding NIH's actions on the previously identified recommendations.

View GAO-22-104467. For more information, contact Jennifer R. Franks at (404) 679-1831 or franksj@gao.gov.

What GAO Found

As GAO reported in June 2021, the U.S. National Institutes of Health (NIH) implemented information security controls—both for its security program and selected systems—intended to safeguard the confidentiality, integrity, and availability of its information systems and information. However, GAO identified numerous control and program deficiencies in the core security functions related to identifying risk, protecting systems from threats and vulnerabilities, detecting and responding to cyber security events, and recovering system operations (see table). GAO made 219 recommendations—66 on the security program and 153 related to system controls—to address these deficiencies.

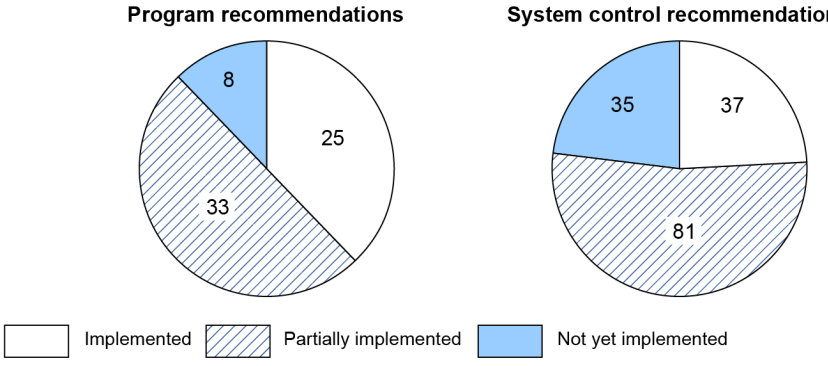
Number of GAO-Identified Information Security Program and Control Deficiencies at the U.S. National Institutes of Health and Associated Recommendations by Core Security Function as of June 2021

Core security function	Number of information security program deficiencies	Number of information security program recommendations	Number of selected system control deficiencies	Number of selected system control deficiency recommendations
Identify	12	26	0	0
Protect	4	6	78	141
Detect	5	11	5	11
Respond	7	16	1	1
Recover	4	7	0	0
Total	32	66	84	153

Source: GAO. | GAO-22-104467

As of June 2021, NIH had made progress in resolving the deficiencies by implementing 25 (about 38 percent) of the 66 information security program recommendations, and 37 (about 24 percent) of the 153 recommendations to address control deficiencies for selected systems. The figure shows the status of NIH's efforts to implement the 219 recommendations.

Status of GAO Recommendations to the U.S. National Institutes of Health as of June 2021



Source: GAO analysis of National Institutes of Health data. | GAO-22-104467

Until NIH fully implements these recommendations and resolves the associated deficiencies, its information systems and information will remain at increased risk of misuse, improper disclosure or modification, and destruction.