December 2018

INFORMATION SECURITY

Significant Progress Made, but CDC Needs to Take Further Action to Resolve Control Deficiencies and Improve Its Program

GAO Highlights

Highlights of GAO-19-70, a report to congressional requesters

Why GAO Did This Study

CDC is responsible for detecting and responding to emerging health threats and controlling dangerous substances. In carrying out its mission, CDC relies on information technology systems to receive, process, and maintain sensitive data. Accordingly, effective information security controls are essential to ensure that the agency's systems and information are protected from misuse and modification.

GAO was asked to examine information security at CDC. In June 2018, GAO issued a limited official use only report on the extent to which CDC had effectively implemented technical 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 2018 report. In addition, for this public report, GAO determined the extent to which CDC has taken corrective actions to address the previously identified security program and technical control deficiencies and related recommendations for improvement. For this report, GAO reviewed supporting documents regarding CDC's actions on previously identified recommendations and interviewed personnel at CDC.

View GAO-19-70. 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.

What GAO Found

As GAO reported in June 2018, the Centers for Disease Control and Prevention (CDC) implemented technical controls and an information security program that were intended to safeguard the confidentiality, integrity, and availability of its information systems and information. However, GAO identified 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 below). GAO made 195 recommendations to address these deficiencies.

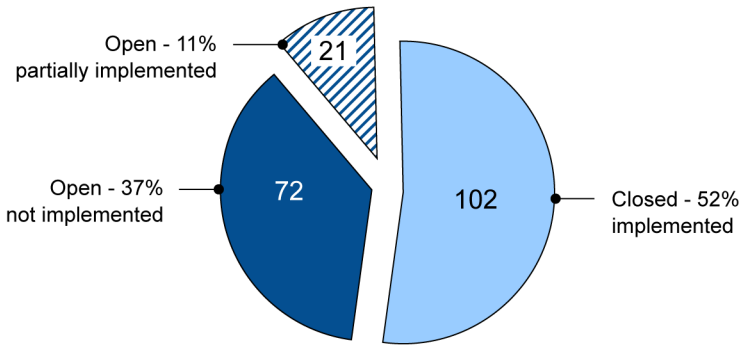
Number of GAO-Identified Technical Control and Information Security Program Deficiencies at the Centers for Disease Control and Prevention and Associated Recommendations by Core Security Function

Core security function	Number of technical control deficiencies	Number of technical control recommendations	Number of information security program deficiencies	Number of information security program recommendations
Identify	0	0	5	5
Protect	85	161	1	1
Detect	8	18	3	3
Respond	1	5	1	1
Recover	0	0	1	1
Total	**94**	**184**	**11**	**11**

Source: GAO. | GAO-19-70

As of August 2018, CDC had made significant progress in resolving many of the security deficiencies by implementing 102 of 184 (about 55 percent) technical control recommendations, and partially implementing 1 of 11 information security program recommendations made in the June 2018 report. The figure shows the status of CDC's efforts to implement the 195 recommendations.

Status of GAO Recommendations to the Centers for Disease Control and Prevention



Source: GAO analysis of CDC data. | GAO-19-70

Additionally, CDC has created remedial action plans to implement the majority of the remaining open recommendations by September 2019. Until CDC 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.