GAO@100 Highlights

Highlights of GAO-21-583, a report to congressional addressees

September 2021

COVID-19

Selected Agencies Overcame Technology Challenges to Support Telework but Need to Fully Assess Security Controls

Why GAO Did This Study

In response to the onset of the COVID-19 pandemic, in March 2020 the Office of Management and Budget directed federal agencies to maximize their use of telework to enable the workforce to remain safe while ensuring that government operations continue. Telework is essential to continuity of operations but also brings added cybersecurity risks.

The *CARES Act* contains a provision for GAO to monitor the federal response to the pandemic. GAO was also asked to examine federal agencies' preparedness to support expanded telework. GAO's objectives were to determine (1) selected agencies' initial experiences in providing the IT needed to support remote access for maximum telework and (2) the extent to which selected agencies followed federal information security guidance for their IT systems that provide remote access.

GAO selected 12 agencies for review that varied in their percentages of reported employee telework use and sent a questionnaire to solicit these agencies' perspectives on the use of IT in transitioning to maximum telework. GAO also reviewed the selected agencies' information security documentation and interviewed relevant officials.

What GAO Recommends

GAO is making a total of nine recommendations to six agencies to document and assess relevant controls, and to fully document remedial actions for systems supporting remote access. The agencies agreed with the recommendations.

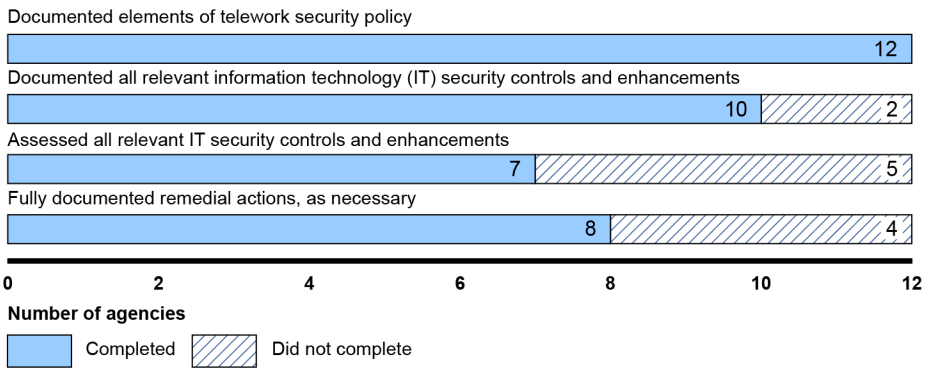
View GAO-21-583. For more information, contact Jennifer R. Franks at (404) 679-1831 or franksj@gao.gov.

What GAO Found

Each of the 12 agencies GAO selected for review had information technology (IT) in place to support remote access for telework during the COVID-19 pandemic. Although the agencies initially experienced IT challenges in supporting remote access for maximum telework, they generally overcame them. For example, seven agencies were challenged in providing sufficient bandwidth to provide remote access for teleworkers, but they increased bandwidth as needed to ensure networks could handle additional remote connections. In addition, while the increased number of remote connections brings additional cybersecurity risks, all of the selected agencies reported that they continued activities intended to help ensure the security of their information and systems.

While the selected agencies had documented elements of a telework security policy, such as permitted telework devices and forms of remote access, not all agencies had fully addressed other relevant federal guidance for securing their systems that support remote access for telework (see figure). Specifically, two agencies had not fully documented relevant IT security controls to protect those systems. In addition, assessments for systems that five agencies relied upon for remote access did not address all relevant controls to ensure the controls were operating effectively. Further, four selected agencies had not fully documented remedial actions to mitigate weaknesses they had previously identified.

Extent to Which 12 Selected Agencies Followed Federal Information Security Guidance in Implementing Their IT Systems That Support Remote Access for Telework



Source: GAO analysis of agency IT security documentation. | GAO-21-583

Although one of the selected agencies subsequently resolved its shortcomings, others had not. For the agencies that did not fully follow federal information security guidance, agency IT security officials stated that these conditions existed for various reasons, such as out-of-date documentation, among others. If agencies do not sufficiently document relevant security controls, assess the controls, and fully document remedial actions for weaknesses identified in security controls, they are at increased risk that vulnerabilities in their systems that provide remote access could be exploited.