May 2020

CYBERSECURITY

Selected Federal Agencies Need to Coordinate on Requirements and Assessments of States

GAO Highlights

Highlights of GAO-20-123, a report to congressional requesters

Why GAO Did This Study

To protect data that are shared with state government agencies, federal agencies have established cybersecurity requirements and related compliance assessment programs. Specifically, they have numerous cybersecurity requirements for states to follow when accessing, storing, and transmitting federal data.

GAO was asked to evaluate federal agencies' cybersecurity requirements and related assessment programs for state agencies. The objectives were to determine the extent to which (1) selected federal agencies' cybersecurity requirements for state agencies varied with each other and federal guidance, and (2) federal agencies had policies for coordinating their assessments of state agencies' cybersecurity.

GAO reviewed four federal agencies that shared data with states and had assessment programs: CMS, FBI, IRS, and SSA. GAO compared, among other things, each agency's cybersecurity requirements to federal guidance and to other selected agencies' requirements; and reviewed federal agencies' policies for conducting assessments. In addition, GAO examined OMB's efforts to foster coordination among federal agencies. GAO also surveyed and received responses from chief information security officers in 50 out of 55 U.S. states, territories, and the District of Columbia to obtain their perspectives.

What GAO Recommends

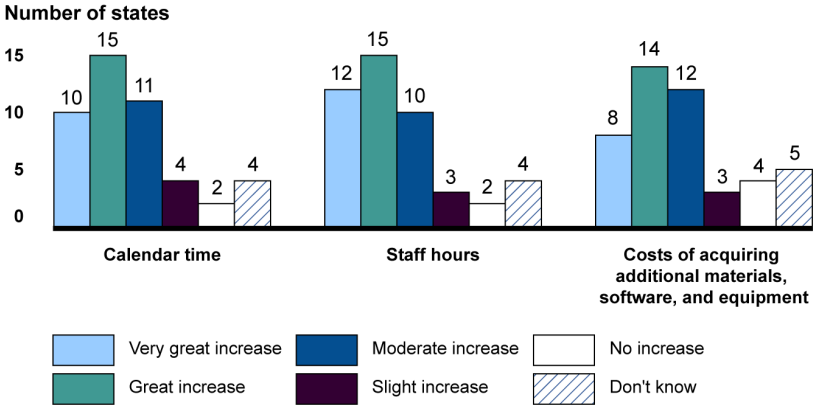
GAO is making 12 recommendations to the four selected agencies and to OMB. Three agencies agreed with the recommendations and one agency (IRS) partially agreed or disagreed with them. OMB did not provide comments. GAO continues to believe all recommendations are warranted.

View GAO-20-123. For more information, contact Vijay D'Souza at (202) 512-6240 or dsouzav@gao.gov.

What GAO Found

Although the Centers for Medicare and Medicaid Services (CMS), Federal Bureau of Investigation (FBI), Internal Revenue Service (IRS), and Social Security Administration (SSA) each established requirements to secure data that states receive, these requirements often had conflicting parameters. Such parameters involve agencies defining specific values like the number of consecutive unsuccessful logon attempts prior to locking out the user. Among the four federal agencies, the percentage of total requirements with conflicting parameters ranged from 49 percent to 79 percent. Regarding variance with National Institute of Standards and Technology guidance, GAO found that the extent to which the four agencies did not fully address guidance varied from 9 percent to 53 percent of total requirements. The variances were due in part to the federal agencies' insufficient coordination in establishing requirements. Although the Office of Management and Budget's (OMB) Circular A-130 requires agencies to coordinate, OMB has not ensured that agencies have done so. Further, while federal agencies' variance among requirements may be justified in some cases because of particular agency mission needs, the resulting impact on states is significant, according to state chief information security officers (see figure).

Extent of Impacts Identified by State Chief Information Security Officers as a Result of Variances in Selected Federal Agencies' Cybersecurity Requirements



Source: GAO analysis of 2019 survey of state chief information security officers. | GAO-20-123

Note: Not all respondents answered all survey questions. The figure is based on 46 responses.

The four federal agencies that GAO reviewed either fully or partially had policies for coordinating assessments with states, but none of them had policies for coordinating assessments with each other. State chief information security officers that GAO surveyed reinforced the need to coordinate assessments by identifying impacts on state agencies' costs, including multiple federal agencies that requested the same documentation. Coordinating with state and federal agencies when assessing state agencies' cybersecurity may help to minimize states' cost and time impacts and reduce associated federal costs. Federal agencies reported spending about $45 million for fiscal years 2016 through 2018 on assessments of state agencies' cybersecurity.