GAO@100
Highlights

Highlights of GAO-22-105024, a report to congressional requesters

Why GAO Did This Study

When the COVID-19 pandemic forced the closure of schools across the nation, many K-12 schools moved from in-person to remote education, increasing their dependence on IT and making them potentially more vulnerable to cyberattacks. Education Facilities, including K-12 schools, is one of the nation's critical infrastructure subsectors. Several agencies have a role in protecting the subsector.

GAO was asked to review cybersecurity in K-12 schools. The objective of this report is to determine the extent that federal agencies have assisted schools in protecting themselves from cyber threats. To do so, GAO identified laws and federal guidance that specify the roles and responsibilities of federal agencies to assist schools in protecting against cyber threats. GAO analyzed documentation of the types of products and services federal agencies have in place to identify, protect, detect, respond, and recover from attacks. In addition, GAO interviewed federal officials about such products and services they offer to K-12 schools.

What GAO Recommends

GAO is making two recommendations for Education to initiate a meeting with CISA to determine how to update its sector-specific plan and determine whether sector-specific guidance is needed. Education concurred with GAO's two recommendations and described actions that it would take to address them.

View GAO-22-105024. For more information, contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov.

October 2021

CRITICAL INFRASTRUCTURE PROTECTION

Education Should Take Additional Steps to Help Protect K-12 Schools from Cyber Threats

What GAO Found

Federal guidance, such as the National Infrastructure Protection Plan (National Plan), specify the roles and responsibilities of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), the Department of Education's Office of Safe and Secure Schools, and the Federal Bureau of Investigation to assist school districts in protecting against cyber threats. These agencies have provided programs, services, and support to assist kindergarten through 12th grade (K-12) schools in defending against cyber threats. Examples of such support include incident response assistance, network monitoring tools, and guidance for parents and students on preparing for the cyber threats that students face online (see table).

Federal Resources for Cyberattacks on Kindergarten through Grade 12 (K-12) Schools

K-12 cyberattack type	Example of a federal resource
Data Breach	The **Department of Education** issued a data breach scenario training kit.
Ransomware	The **Cybersecurity and Infrastructure Security Agency** issued a guide, for ransomware prevention and response.
Business Email Compromise	The **Federal Bureau of Investigation** issued a notice on the use of malicious emails to compromise the business operations of organizations, and potential mitigations.
Distributed Denial-of-Service	The **Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigations,** and the **Multi-State Information Sharing and Analysis Center** jointly issued an alert, which described the threat that distributed denial-of-services attacks can pose to K-12 schools and potential mitigations.
Video Conferencing Disruptions	The **Cybersecurity and Infrastructure Security Agency** issued a document detailing the vulnerabilities in video conferencing and potential mitigations.

Source: GAO analysis of federal and non-federal documents. | GAO-22-105024

As the lead for the education subsector, the Department of Education is responsible for (1) developing and maintaining a sector-specific plan to address cybersecurity risks at K-12 schools, and (2) determining the need for sector-specific guidance. The Education Facilities plan was developed and issued in 2010. Since then, the cybersecurity risks facing the subsector have substantially changed. Among other things, schools have increasingly reported ransomware and other cyberattacks that can cause significant disruptions to school operations, thus highlighting the importance of securing K-12 schools' IT systems. According to data from K-12 Security Information Exchange, schools publicly reported 62 ransomware incidents in 2019, compared to 11 ransomware incidents reported in 2018. However, Education has not updated its 2010 plan and has not determined whether sector-specific guidance is needed for K-12 schools to help protect against cyber threats. Education officials stated that the department has not updated the sector plan and not determined the need for sector-specific guidance because CISA has not directed it to do so. However, as previously stated, the department is responsible for updating its sector plan and determining the need for guidance. As a result, K-12 schools are less likely to have the federal products, services, and support that can best help protect them from cyberattacks.