October 2022

CRITICAL INFRASTRUCTURE PROTECTION

Additional Federal Coordination Is Needed to Enhance K-12 Cybersecurity

Accessible Version

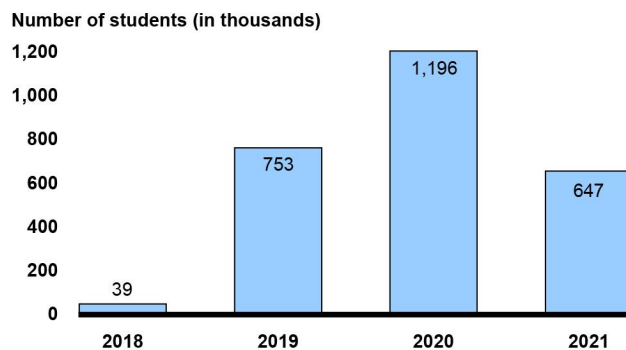# CRITICAL INFRASTRUCTURE PROTECTION

Additional Federal Coordination Is Needed to Enhance K-12 Cybersecurity

Why GAO Did This Study

The COVID-19 pandemic forced schools across the nation to increase their reliance on IT to deliver educational instruction to students. This amplified the vulnerability of K-12 schools to potentially serious cyberattacks. Several federal agencies have a role in enhancing the protection of our nation's critical infrastructure, which includes the Education Facilities Subsector.

GAO was asked to review cybersecurity in K-12 schools. The objectives of this report are to (1) determine what is known about the impact of cyber incidents, and (2) determine the extent to which key federal agencies coordinate with other federal and nonfederal entities to help K-12 schools combat cyber threats.

To do so, GAO analyzed publicly reported K-12 cyber incidents and related documentation. In addition, GAO identified law and federal guidance that establish roles and responsibilities for coordinating K-12 cybersecurity. GAO also interviewed officials from federal agencies and selected state-level and local-level school-related organizations on the impact of cyber incidents and level of federal cybersecurity support received.

What GAO Recommends

GAO is making three recommendations to Education and one to DHS to improve coordination of K-12 schools' cybersecurity and to measure the effectiveness of products and services. Education concurred with one recommendation and partially concurred with two; DHS concurred with its recommendation. GAO continues to believe all recommendations are warranted.

What GAO Found

Kindergarten through grade 12 (K-12) schools have reported significant educational impact due to cybersecurity incidents, such as ransomware attacks. Cyberattacks can also cause monetary losses for targeted schools due to the downtime and resources needed to recover from incidents. Officials from state and local entities reported that the loss of learning following a cyberattack ranged from 3 days to 3 weeks, and recovery time ranged from 2 to 9 months. While the precise national magnitude of cyberattacks on K-12 schools is unknown, the research organization Comparitech reported the number of students affected by ransomware attacks between 2018 and 2021 (see figure).

Number of U.S. Students Affected by Ransomware Attacks on K-12 Schools and School Districts, 2018-2021

Number of students (in thousands)

Source: GAO analysis of Comparitech study on K-12 school ransomware attacks. | GAO-23-105480

Federal guidance, such as the National Infrastructure Protection Plan (National Plan), establishes roles and responsibilities for the protection of the nation's critical infrastructure, including the Education Subsector. Specifically, the Department of Education (Education) is the lead agency, or sector risk management agency, for the subsector. As such, Education and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) are to coordinate K-12 cybersecurity efforts with federal and nonfederal partners. In addition, the FBI is to provide criminal investigative support.

Education and CISA offer cybersecurity-related products and services to K-12 schools, such as online safety guidance. However, they otherwise have little to no interaction with other agencies and the K-12 community regarding schools' cybersecurity. This is due in part to Education not establishing a government coordinating council, as called for in the National Plan. Such a council can facilitate ongoing communication and coordination among federal agencies and with the K-12 community. This, in turn, can enable federal agencies to better address the cybersecurity needs of K-12 schools. Regarding the products and services they do offer to schools, Education and CISA do not measure their effectiveness. Doing so would provide further input on the needs of the schools.

United States Government Accountability Office

Contents

Figures

Abbreviations

CISA	Cybersecurity and Infrastructure Security Agency
DDoS	distributed denial-of-service
DHS	Department of Homeland Security
Education	Department of Education
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
ISAC	Information Sharing and Analysis Center
K-12	kindergarten through grade 12
K12 SIX	K-12 Security Information Exchange
MS-ISAC	Multi-State Information Sharing and Analysis Center
National Plan	National Infrastructure Protection Plan
NDAA	National Defense Authorization Act
NIST	National Institute of Standards and Technology
OSSS	Office of Safe and Supportive Schools
PPD	Presidential Policy Directive
SRMA	sector risk management agency
SSP	sector-specific plan

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.
Washington, DC 20548

October 20, 2022

Congressional Requesters

Many kindergarten through grade 12 (K-12) schools moved from in-person to remote education when the COVID-19 pandemic forced the closure of schools across the nation in March 2020.[1] Remote education increased K-12 schools' dependence on IT such as laptops, wireless internet access, and computer cameras and microphones. Such heavy reliance on IT to deliver educational instruction has increased the vulnerability of K-12 schools to potentially serious cyberattacks. From 2018 to April 2022, schools in most states reported an increase in cyberattacks.

Ensuring the cybersecurity of the nation has been on GAO's High Risk List since 1997. In 2003, we expanded this area to include the protection of critical cyber infrastructure, which includes the Education Facilities Subsector as well as other sectors and subsectors.[2] In September 2018, we issued an update that identified actions needed to address cybersecurity challenges facing the nation, including the development of a more comprehensive national strategy and better oversight of national cybersecurity.[3] In our March 2021 update, we identified ensuring the cybersecurity of the nation as a high-risk area needing urgent actions by federal agencies and other entities.[4]

You asked us to review the cybersecurity-related coordination between federal agencies and K-12 schools. Our objectives were to (1) determine

---

[1]K-12 includes all public, private, and charter schools from kindergarten through 12th grade. The scope of our review was limited to K-12 public and private schools, which we refer to as "K-12 schools" in this report.

[2]GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, GAO-17-317 (Washington, D.C.: Feb. 16, 2017). The Education Facilities Subsector includes K-12 schools, higher education institutions, and business and trade schools, and falls under the Government Facilities Sector. The subsector includes facilities that are owned by both government and private sector entities.

[3]GAO, *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, GAO-18-622 (Washington, D.C.: Sept. 6, 2018).

[4]GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, GAO-21-119SP (Washington, D.C.: Mar. 2, 2021).

what is known about the impact of cyber incidents on school districts and (2) determine the extent to which key federal agencies coordinate with other federal and nonfederal entities to help K-12 schools combat cyber threats. This is the second of two reports responding to your request. The first report focused on the extent to which federal agencies have assisted schools in protecting themselves from cyber threats.[5]

To address the first objective, we collected and analyzed documentation, reports, and data regarding the reported impact of cyber incidents at K-12 schools. We conducted semi-structured interviews with officials from selected K-12 school districts, state-level organizations, and one state-level association, to obtain information regarding the impact of cyber incidents on their school systems. In total, we interviewed officials from 18 state and local entities knowledgeable about K-12 cybersecurity.[6] We analyzed the K-12 school districts and state-level organizations' views to identify trends.

To select the states and school districts included in our review, we collected and analyzed unpublished data from the K-12 Security Information Exchange (K12 SIX) regarding publicly reported significant K-12 cyber incidents from January 2018 to December 2021.[7] We also collected data from the Department of Education's (Education) Common Core of Data regarding student population by state during the 2019-2020 school year. We analyzed the K12 SIX data to determine the number of incidents that occurred in each state during that time frame and organized the states by the most reported state-wide cyber incidents to the least. We took steps to ensure the reliability of the incident data by analyzing the sources and independently confirming they were linked to reported cyber incidents because the selection data included only publicly and voluntarily reported incidents.

---

[5]GAO, *Critical Infrastructure Protection: Education Should Take Additional Steps to Help Protect K-12 Schools from Cyber Threats*, GAO-22-105024 (Washington, D.C.: Oct. 13, 2021).

[6]The state and local entities knowledgeable about K-12 cybersecurity included K-12 school districts, IT and cybersecurity organizations, and one state-level association from selected states: California, Pennsylvania, North Carolina, Connecticut, Texas, and Michigan.

[7]K12 SIX is a national nonprofit information-sharing organization that assists its members from the K-12 community in protecting from cybersecurity threats. School districts are not required to report their incidents to K12 SIX, thus the incident data represent a portion of the actual total.

We selected three states by identifying the top 10 with the most reported K-12 cyber incidents. From those top 10 states, we selected three states based on student population, selecting the most and least populated, and one state from the middle range of the group to include California, Pennsylvania, and North Carolina. In addition, based on referrals from those states, we interviewed officials from Connecticut, Texas, and Michigan because of their reported knowledge about K-12 cybersecurity.

Also, to select school districts within the three states, we ranked each state's school districts by student population based on Education's Common Core of Data during the 2019-2020 school year. We then selected and contacted three school districts in each state of California, Pennsylvania, and North Carolina. We determined the school districts to contact based on student population. Of those contacted, officials from seven school districts agreed to participate in our study.

In addition, we collected and analyzed public and nonpublic data from Comparitech regarding the reported and estimated impacts of ransomware incidents at K-12 school districts from January 2018 to December 2021.[8] We analyzed the data to identify trends in the total downtime and recovery time that schools attacked with ransomware experienced as well as trends in the costs of downtime that those schools experienced.

We assessed the reliability of the data by interviewing Comparitech officials regarding their methodology for the study. Their methodology included the sources used to collect the data and steps taken to ensure the data were entered accurately. We found that the data Comparitech provided were reliable for the purpose of summarizing results as background to provide context for our findings.

---

[8]Comparitech is a research organization that provides information, tools, reviews, and comparisons to readers to help improve their cybersecurity and privacy online. They have identified and reported on data breaches and incidents impacting online users. They also test and review products including virtual private networks, password managers, identity theft protection, antivirus software, network monitoring tools, and firewalls. The Comparitech data used to describe the reported cost impact of cyber incidents on K-12 schools include only voluntarily reported incidents. In addition, Comparitech provided us with data that were not publicly released regarding ransomware incidents and their impacts on K-12 school districts. For these data, Comparitech calculated the average estimates of downtime and cost of downtime for schools in which no figures were publicly reported. Comparitech used a simple estimation method that treats all schools, regardless of size or location, in a similar manner.

To address the second objective, we examined relevant law and federal guidance, such as the National Defense Authorization Act (NDAA) for Fiscal Year 2021 and the National Infrastructure Protection Plan (National Plan) that establish roles and responsibilities for the protection of the nation's critical infrastructure, including the Education Subsector.[9] Based on our analysis of relevant federal law and guidance, Education and the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) have responsibilities for coordinating with federal and nonfederal partners to provide assistance to school districts. In addition, the Federal Bureau of Investigation (FBI) is responsible for investigating cyberattacks and intrusions across critical infrastructure sectors, including the Education Subsector.

Further, we examined the Telecommunications Act of 1996 that specifies authorities under which the Federal Communications Commission (FCC) is to provide assistance to school districts.[10] We collected and analyzed documents and interviewed officials from Education, CISA, the FBI, and the FCC about the actions taken to coordinate with each other and with other federal agencies and nonfederal entities.

We then compared these agencies' efforts to provide assistance to K-12 school districts to coordination requirements set forth in applicable law and federal guidance to determine the extent to which agencies are meeting requirements. In addition, we conducted semi-structured interviews with officials from selected K-12 school districts and from state-level IT and cybersecurity organizations that provide support to K-12 school districts. Based on referrals from our original selection of states, we also interviewed officials from Connecticut, Texas, and Michigan because of their knowledge about K-12 cybersecurity.

We obtained testimonial evidence from state and local school officials and organizations that provide support to schools about whether they used

---

[9]Department of Homeland Security, *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: December 2013). The National Plan lists the Department of Education as the sector-specific agency for the Education Facilities Subsector. Presidential Policy Directive (PPD) 21 establishes requirements for sector-specific agencies and DHS. The Fiscal Year 2021 NDAA renamed the term "sector-specific agency" to "sector risk management agency" (SRMA), listed responsibilities for those agencies, and addressed the designation of critical infrastructure sectors. The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Fiscal Year 2021 NDAA), Pub. L. No. 116-283, § 9002, 134 Stat. 4768 (Jan. 1, 2021).

[10]Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56, 72 (1996).

federal resources and other assistance regarding cybersecurity, including help received following a cyber incident, and their views of the support they received. We further obtained information on current cybersecurity issues and challenges at K-12 schools and obtained views from state and local-level schools and organizations on how the federal government could better address cybersecurity issues at K-12 schools. Appendix I discusses our objectives, scope, and methodology in greater detail.

We conducted this performance audit from October 2021 to October 2022 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

The U.S. critical infrastructure refers to systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on our nation's security, economic stability, public health or safety, or any combination of these factors. National policy has identified 16 critical infrastructure sectors, including the Government Facilities Sector with the Education Facilities Subsector.[11] The Education Facilities Subsector includes facilities that are owned by both government and private-sector entities and covers pre-kindergarten through 12th grade schools, institutions of higher education, and business and trade schools.[12]

IT systems supporting our nation's critical infrastructure are inherently at risk. Within the Education Facilities Subsector, systems and networks used by schools are often interconnected with other internal and external systems and networks, including the internet. In addition, schools,

---

[11]The other sectors include: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; Transportation Systems; and Water and Wastewater Systems.

[12]We limited the scope of our review to public and private K-12 schools.

districts, states, and educational technology vendors[13] collect and store a range of information about students in these systems and networks. This information includes grades, test scores, addresses, telephone numbers, emails, Social Security numbers, and medical information. With greater connectivity among these systems and networks, threat actors attack these systems for financial gain, to disrupt classes, or for other potentially destructive purposes.[14]

Federal law, policy, and public-private plans establish roles and responsibilities for the protection of critical infrastructure, including the Education Facilities Subsector. For example, the Education Facilities Sector-Specific Plan (SSP), an annex to the Government Facilities SSP, designates Education as the sector risk management agency (SRMA) for the Education Facilities Subsector. Key laws, policies, and plans are discussed in detail in appendix II.

We previously reported on the roles and responsibilities of Education, CISA, and the FBI in assisting the Education Subsector in protecting and defending against, and responding to cyber threats.[15] Within Education, the department's Office of Safe and Supportive Schools (OSSS) fulfills this role. As such, OSSS is responsible for coordinating with federal partners to address risk management for schools, including cybersecurity risks. OSSS officials stated that they work with other Education offices to fulfill these responsibilities. In addition, OSSS is to collaborate with nonfederal partners within the Education Subsector, including critical infrastructure owners and operators, regulatory agencies, and others. Further, Education provides a variety of products and services. For example, Education offers resources for K-12 schools and institutions of higher education through its technical assistance centers, including tabletop exercises and guidance for parents and students on preparing for cyber threats online.

CISA is the lead federal agency for asset response and national coordinator for the protection of critical infrastructure. As such, CISA is responsible for, among other things, coordinating the overall federal effort to promote the security and resilience of critical infrastructure. In addition,

---

[13]Educational technology vendors provide technological resources to schools such as hardware and software to support teaching and learning in an educational setting.

[14]GAO, *Data Security: Recent K-12 Data Breaches Show That Students Are Vulnerable to Harm*, GAO-20-644 (Washington, D.C.: Sept. 15, 2020).

[15]GAO-22-105024.

CISA provides a variety of products and services such as training exercises, cybersecurity awareness webinars, network monitoring tools, and cyber threat alerts.

The agency is in charge of developing and implementing information sharing programs to help spread awareness about cyber threats, protective measures, and response tactics. CISA is also responsible for conducting a study of how cybersecurity risks impact schools and developing voluntary recommendations for addressing those risks.

The FBI is the lead federal agency for threat response activities.[16] Its responsibilities entail investigating cyberattacks and intrusions across critical infrastructure sectors, including the Education Subsector.[17] The FBI is a focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations within the federal government, as appropriate. In addition to conducting threat response activities, the FBI issues information and alerts about specific cyber threats targeting state, local, tribal, and territorial governments, to include K-12 entities. The FBI coordinates with CISA on many of these alerts.

In regard to K-12 schools, FBI officials stated that typically FBI headquarters organizations are responsible for coordinating primarily with national level organizations. FBI officials also said that the 56 FBI field offices are responsible for outreach to schools that are victims of a cyber incident and for performing investigations of those incidents.

In addition to Education, CISA, and the FBI, the FCC has a role in helping to ensure access to affordable broadband for schools, libraries, health care providers, and rural and low-income consumers.[18] For example, the

---

[16]Presidential Policy Directive 41 designates the FBI as the lead federal agency for threat response activities, such as investigation of cyberattacks and intrusions across critical infrastructure sectors. The White House, United States Cyber Incident Coordination, Presidential Policy Directive 41 (Washington, D.C.: July 26, 2016).

[17]FBI officials said that the FBI investigates cyberattacks and seeks to identify those responsible. In addition, the officials said that during the course of fulfilling these responsibilities, the FBI's ability to provide support is based upon the circumstances of the incident, which include the amount and type of information provided by the victim and the victim's level of cooperation.

[18]The FCC regulates interstate and international communications by radio, television, wire, satellite, and cable through the United States, and is also responsible for enforcing communications law and regulations. The FCC's major statutory authority is the Communications Act of 1934, Pub. L. No. 73-416, 48 Stat. 1064 (1934), and amended by the Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996).

FCC provides support to K-12 school districts through the schools and libraries universal service support program, commonly known as the E-rate program. The program provides funding to K-12 schools to acquire eligible telecommunications services, telecommunications, internet access, internal connections, basic maintenance, and managed internal broadband services. The E-rate program can cover the cost of certain cybersecurity services such as basic firewall protection included in the internet access service provided by the school's internet service provider, as well as separately priced components for basic firewall protection.

Beyond federal roles and responsibilities, other organizations provide school districts with cybersecurity support and services at the state level. They include state education agencies, county education offices, and state IT and cybersecurity agencies. These organizations may provide school districts with workshops and training, information sharing, cybersecurity services such as network scanning, and assistance following a cyber incident.

A Variety of Cyber Threats Can Impact the Education Facilities Subsector

K-12 schools across the nation face a range of cybersecurity dangers from various threat actors using a variety of different methods. The threat actors may be motivated by the promise of monetary gain, by the desire to steal data, or simply to cause disruption of K-12 classes. The FBI, CISA, and the Multi-State Information Sharing and Analysis Center (MS-ISAC)[19] have noted that threat actors target K-12 remote education to cause disruptions and steal data.[20] In addition, insiders, including students, staff, and vendors, can pose a threat to K-12 security. Table 1 summarizes the various types of threat actors.

---

[19]The MS-ISAC is an independent, nonprofit organization that DHS designated in 2010 as the cybersecurity ISAC for state, local, tribal, and territorial governments. It provides services and information sharing to enhance state, local, tribal, and territorial governments' ability to prevent, protect against, respond to, and recover from cyberattacks and compromises.

[20]Cybersecurity and Infrastructure Security Agency, *Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data*, AA20-345A (Dec. 10, 2020), accessed March 15, 2022, https://us-cert.cisa.gov/ncas/alerts/aa20-345a.

Table 1: Cybersecurity Threat Actors

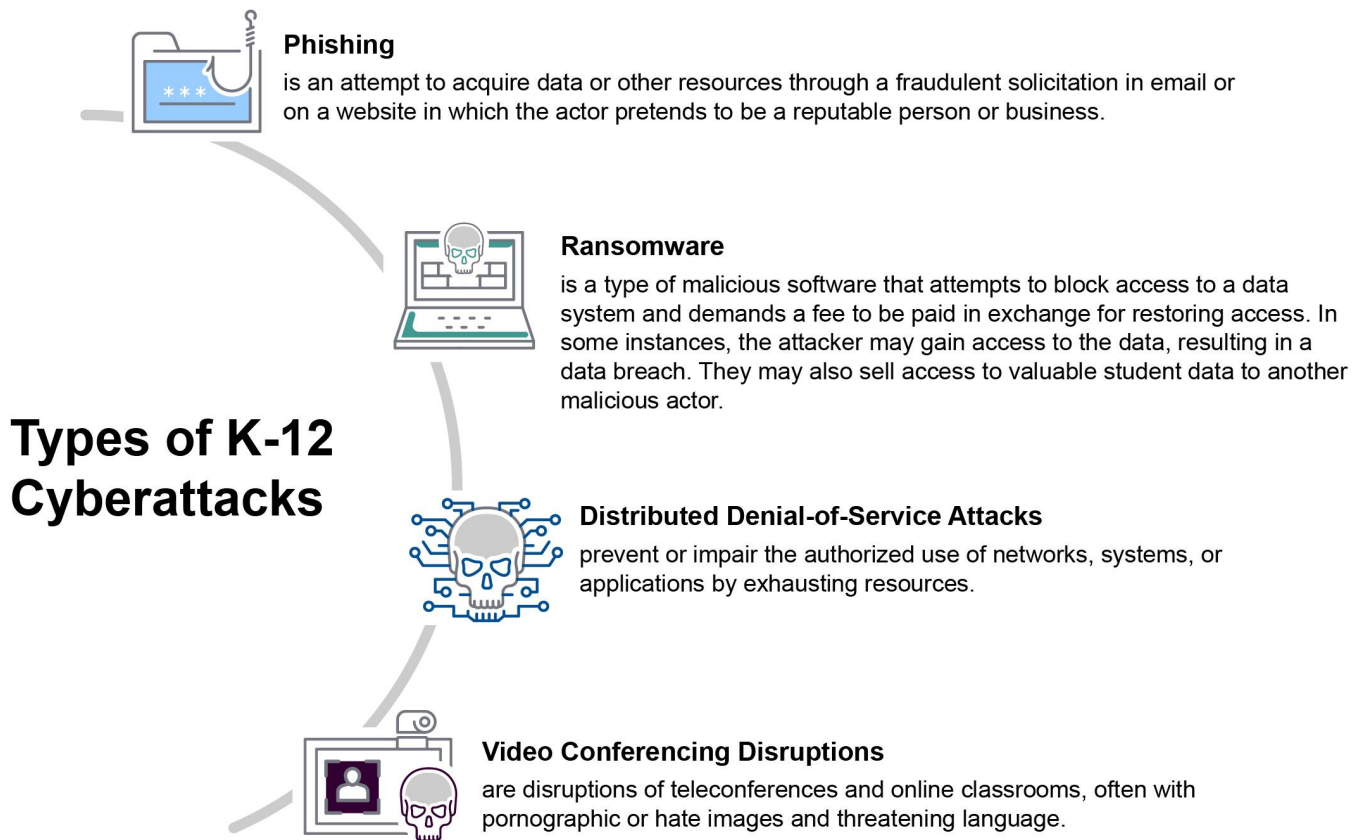| Threat actor	Description
Criminal groups	Criminal groups, including organized crime organizations, seek to use cyberattacks for monetary gain. According to the Department of Homeland Security's *2020 Homeland Threat Assessment,* cybercriminals increasingly target critical infrastructure to generate profit. The assessment also states that criminal organizations often use ransomware—malicious software used to deny access to systems or data—against critical infrastructure entities at the state and local levels by exploiting gaps in cybersecurity.
Insiders	Insiders are individuals with authorized access to an information system or enterprise who have the potential to cause harm, wittingly or unwittingly, through destruction, disclosure, or modification of data or through denial of service. Insiders could include system administrators or other knowledgeable employees with privileged access to critical systems, students with authorized access, or contractors with limited system knowledge.
Nations	Nations, including groups or programs sponsored or sanctioned by nation states, use cyber tools as part of their information gathering and espionage activities. According to the Director of National Intelligence's *2019 Worldwide Threat Assessment of the U.S. Intelligence Community* and the *2020 Homeland Threat Assessment,* China and Russia pose the greatest cyberattack threats. Of particular concern, both nations have the ability to launch cyberattacks that could disrupt or damage critical infrastructure.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, inflict mass casualties, weaken the economy, and damage public morale and confidence. Terrorists could create disruptions by executing denial-of-service attacks against poorly protected networks.

Sources: Summary of GAO, Electricity Grid Cybersecurity: DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems, GAO-21-81 (Washington, D.C.: Mar. 18, 2021), and other relevant federal documents. | GAO-23-105480

These threat actors conduct cyberattacks using various methods, including ransomware, video conferencing disruptions, denial-of-service attacks, and phishing. In 2021, we reported that K-12 schools and their vendors are increasingly subject to data breaches.[21] From 2018 to the present, schools in most states have reported cyberattacks on their systems. COVID-19 remote learning protocols increased school districts' usage of IT systems and increased the potential for a cyberattack as threat actors view schools as opportunistic targets. Figure 1 describes cyberattack methods that have been used against K-12 schools.

---

[21]GAO-22-105024.

Figure 1: Cyberattacks Used Against Kindergarten through Grade 12 Schools

Types of K-12 Cyberattacks

Phishing

is an attempt to acquire data or other resources through a fraudulent solicitation in email or on a website in which the actor pretends to be a reputable person or business.

Ransomware

is a type of malicious software that attempts to block access to a data system and demands a fee to be paid in exchange for restoring access. In some instances, the attacker may gain access to the data, resulting in a data breach. They may also sell access to valuable student data to another malicious actor.

Distributed Denial-of-Service Attacks

prevent or impair the authorized use of networks, systems, or applications by exhausting resources.

Video Conferencing Disruptions

are disruptions of teleconferences and online classrooms, often with pornographic or hate images and threatening language.

Source: GAO analysis of federal and nonfederal documents; images: marinashevchenko/stock.adobe.com. | GAO-23-105480

Education and CISA Have Taken Limited Steps to Address Prior GAO Recommendations Related to K-12 Cybersecurity

In October 2021, we reported that Education had not updated the 2010 sector-specific plan (SSP) and had not determined whether sector-specific guidance was needed for K-12 schools to help protect against cyber threats.[22] To address these issues, we recommended that Education initiate a meeting with CISA to (1) determine how to update its

---

[22]GAO-22-105024.

SSP and (2) determine whether sector-specific guidance was needed. At the time, Education concurred with our two recommendations.

Education officials stated that an initial meeting was held in July 2022 between Education and CISA officials to discuss how to initiate the process for updating the Education Facilities Subsector SSP. Officials also stated that future meetings had been scheduled to further discuss updating the SSP. The officials also said that they had not discussed the need for sector-specific guidance with CISA because they were taking other steps that they thought were necessary before determining the need for specific guidance. For example, the officials said they were inventorying all of the products and services that are available across the department's offices in an effort to identify gaps in the products and services they provide to K-12 school districts. Without an up-to-date plan reflecting current risks and operational circumstances, K-12 schools continue to be less likely to have the federal support that can help protect them from cyberattacks. We will continue to monitor Education's efforts to address our recommendations.

Cyber Incidents Significantly Impact K-12 Schools, but Precise National Magnitude Is Unknown

Although the total number of K-12 cybersecurity incidents is unknown, research from federal and private sector sources show that cyber threats are escalating. In addition, these incidents can significantly impact schools' ability to continue operations and can cause learning and monetary loss due to downtime and the time it takes schools to recover from an incident. Officials from state and local-level school districts and IT organizations reported experiencing ransomware (seven), distributed denial-of-service (DDoS) attacks (three), phishing (three), and data theft (two). While some of these officials noted that their individual states have requirements to centrally report cyber-related incidents, the precise national magnitude of the impact of cyber incidents on K-12 schools is unknown due to limited reporting requirements.

Data Show Cyberattacks at K-12 Schools Are Increasing

The total number of cyberattacks at K-12 schools is unknown due to potential reluctance to report being a victim, fear of being targeted again, and cyber insurance policy restrictions, among other things, according to

three state and local-level officials. In addition, there is not a single federal or nonfederal source for the total number of cyberattacks on schools.

Nonetheless, research from several federal and private sector sources indicate that cyber threats have escalated over time, and are becoming more sophisticated and pervasive. For example, according to data from K12 SIX, K-12 schools publicly reported 62 ransomware[23] incidents in 2021, compared to 50 ransomware incidents reported in 2020 and 62 ransomware incidents reported in 2019.[24] In addition, the data showed that 55 percent of all data breaches at K-12 schools between 2016 and 2021 were carried out on schools' vendors. These attacks further increased during the COVID-19 pandemic.

In addition, according to data from the MS-ISAC, reported ransomware incidents against K-12 schools increased significantly in August and September 2020. Fifty-seven percent of all ransomware incidents reported to the MS-ISAC involved K-12 schools, compared to 28 percent of reported ransomware incidents around the end of the 2019-2020 school year (January through July 2020).

K-12 Schools Face Significant Impacts from Cyber-related Incidents

Cybersecurity incidents at K-12 schools can significantly impact the schools' ability to continue operations and can cause learning and monetary loss. Publicly reported examples of K-12 cyber-related incidents show the impact on K-12 schools. Examples of these impacts include:

- In December 2021, a vendor for Chicago Public Schools was a victim of a ransomware attack in which more than 500,000 students' and

---

[23]Ransomware is a type of malicious software that attempts to block access to a data system and demands a fee to be paid in exchange for restoring access. In some instances, the attacker may gain access to the data, resulting in a data breach. Attackers may also sell access to valuable student data to another malicious actor.

[24]K12 SIX began collecting data on cyber incidents, including ransomware, in 2016 and does not have data prior to that year.

staff members' personal information was disclosed.[25] The data included students' names, schools, dates of birth, genders, school identification numbers, state student identification numbers, and course information from previous school years.

- In February 2021, Winthrop Public Schools was a victim of a denial-of-service attack that disrupted learning and teaching on the district's networks and web-based systems, including email, learning platforms and video conferencing services.[26]

- In September 2020, Miami-Dade County Public Schools was a victim of a series of denial-of-service attacks that disrupted learning and teaching on the district's networks and web-based systems.[27]

In addition to the publicly reported incidents, officials representing school districts and state and local organizations supporting schools reported that the most significant cyber threats currently facing K-12 school districts include data theft, DDoS attacks, phishing, and ransomware. Officials said that in many cases DDoS attacks were conducted by students to hinder standardized testing. More specifically:

- Texas officials reported they were aware of Texas schools that experienced seven ransomware and three DDoS attacks, two data breaches, and one phishing incident in 2020.[28] According to an official, one school district in Texas reported experiencing DDoS attacks on the first day of classes and another district paid a $500,000 ransomware payment.

- Connecticut officials reported a school district had to shut down for 3-4 days due to a cybersecurity incident. Another incident involved a

---

[25]Chicago Public Schools, "Breach Notification for May 20, 2022" (Chicago, IL: May 20, 2022), accessed July 20, 2022, https://www.cps.edu/about/policies/student-online-personal-protection-act/breach-notifications/.

[26]The Town of Winthrop Massachusetts, "Winthrop Officials Investigating Cyber Attack on Town, School Servers" (Winthrop, MA: Feb. 5, 2021), accessed July 19, 2022, https://www.town.winthrop.ma.us/home/news/winthrop-officials-investigating-cyber-attack-town-school-servers.

[27]Miami-Dade County Office of Communications, "Arrest Made in Cyber Attacks Against M-DCPS" (Miami, FL: Sept. 3, 2020), accessed July 19, 2022, https://news.dadeschools.net/cmnc/new/30657.

[28]According to the Texas official, the state of Texas only requires schools to report data breach incidents. Therefore, other types of incidents (e.g., DDoS, phishing, and ransomware) may be underreported.

Connecticut school district being reinfected 2-3 days after an incident, due to the school district's cybersecurity insurance company not providing sufficient recovery response, according to the school district.

- California officials reported experiencing DDoS attacks conducted by students. The officials reported that students could obtain software for $30-$50 on the internet and cause a 20- to 30-minute attack.

In addition, officials from more than half of the 18 state and local entities knowledgeable about K-12 cybersecurity reported experiencing impacts of downtime (eight), recovery time (one), and monetary loss (nine) due to cybersecurity incidents.[29] Some of these officials reported that the loss of learning (downtime) ranged from 3 days to 3 weeks, and some experienced significant incident recovery times that ranged from 2 to 9 months due to schools' limited resources. For example, an official from a California school district said that it took their school district about 2 weeks to recover from a ransomware incident that resulted in 2 weeks' worth of data being lost. In addition, officials reported that the monetary loss school districts experienced from downtime and recovery time ranged from $50,000 to $1 million due to expenses caused by a cyber incident (e.g., cyber insurance deductibles, enhancement of cybersecurity to prevent future attacks, and replacement of hardware).

Research Shows Ransomware Attacks Affected a Large Number of Students and Resulted in Lengthy Downtimes

Comparitech conducted research on the impact of ransomware attacks at K-12 schools between 2018 and 2021.[30] The research found that millions of students were impacted, and school districts experienced both lengthy downtimes and substantial monetary losses. Figure 2 shows the number of students reported as being affected by ransomware incidents each year from 2018 to 2021.

---

[29]These responses are not mutually exclusive and an entity may have responded to more than one of these categories.

[30]Comparitech Limited, *Ransomware attacks on US schools and colleges cost $6.62bn in 2020* (accessed on Nov. 4, 2021), https://www.comparitech.com/blog/information-security/school-ransomware-attacks/. Note: Comparitech updates this article periodically and treats it as a living document. Comparitech allowed GAO access to its data at the time of our research; some of the data were not reflected in the article.

Figure 2: Number of Students Reportedly Affected by Ransomware Attacks on U.S. K-12 Schools and School Districts, 2018-2021

Number of students (in thousands)
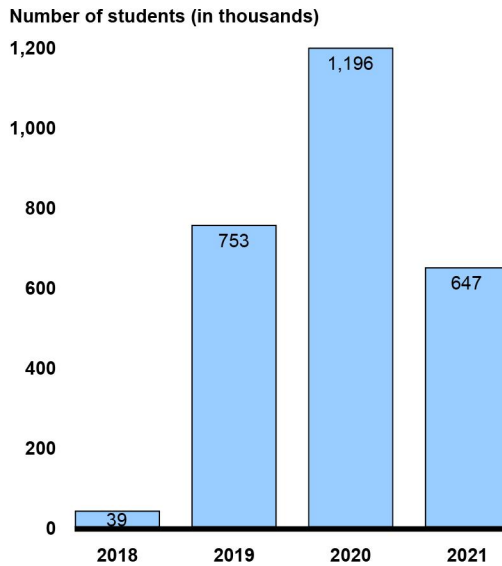
Source: GAO analysis of Comparitech study on K-12 school ransomware attacks. | GAO-23-105480

Comparitech also found that the total downtime increased at school districts that experienced a ransomware attack from 2018 to 2019.[31] The annual combined reported and total estimated downtime for schools and school districts due to ransomware attacks annually from January 2018 through December 2021 is shown in figure 3.[32]

---

[31]Comparitech provided GAO with data that were not publicly released regarding ransomware incidents and their impacts on K-12 school districts.

[32]The Comparitech data used to describe the reported downtime on K-12 schools include only voluntarily reported incidents. In addition, for incidents that did not report downtime, Comparitech calculated the average estimates of downtime for schools for which there were no publicly reported downtime figures. Comparitech used a simple estimation method that treated school districts of all sizes in a similar way.

Figure 3: Reported and Estimated U.S. School/School District Downtime from Ransomware Attacks

Downtime (in days)
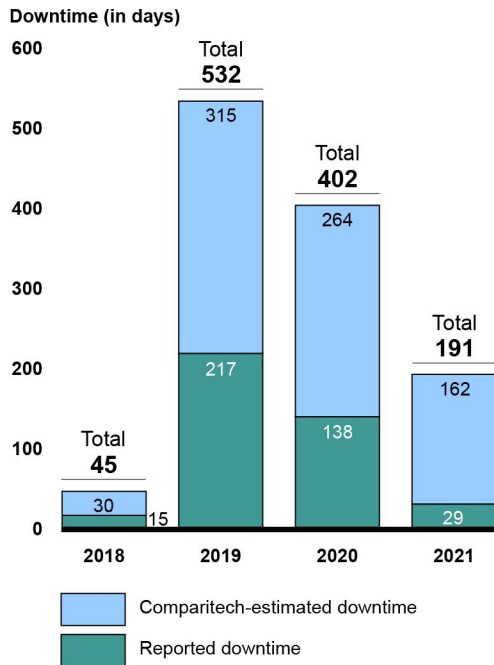
Source: GAO analysis of Comparitech study on K-12 school ransomware attacks. | GAO-23-105480

In addition, according to Comparitech's research, the annual combined estimated downtime costs to schools and school districts due to ransomware attacks from 2018 to 2021 peaked in 2019 at $6.64 billion. The annual combined estimated downtime costs to schools and school districts are shown in figure 4.[33] These costs are drawn from Comparitech's research on ransomware attacks at K-12 school districts.

[33]Schools did not report data on the costs of downtime from these ransomware attacks. For these data, Comparitech calculated the average estimates of downtime costs for schools. Comparitech used a simple estimation method that treated school districts of all sizes in a similar way.

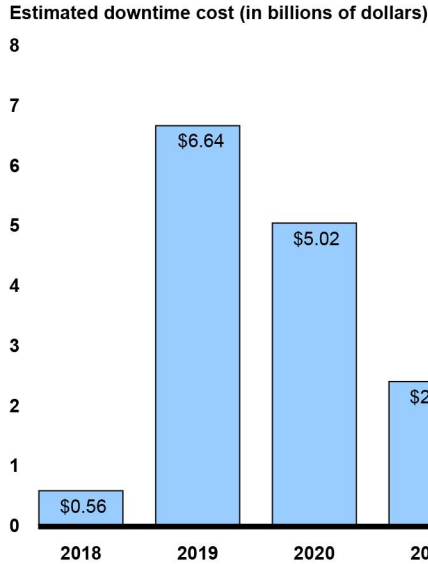**Figure 4: Estimated U.S. School/School District Costs of Downtime from Ransomware Attacks**

Estimated downtime cost (in billions of dollars)

Year	Cost
2018	$0.56
2019	$6.64
2020	$5.02
2021	$2.38

Source: GAO analysis of Comparitech study on K-12 school ransomware attacks. | GAO-23-105480

Limited Cyber Incident Reporting Hinders Understanding of National Magnitude, but Recent Legislation Calls for Increased Reporting

The precise national magnitude of the impact of cyber incidents on K-12 schools is unknown, in part, due to limited reporting requirements. There are no federal requirements for school districts to report incidents to federal agencies and only two states under our review had established requirements to centrally report cyber-related incidents. More specifically, of the officials from the 18 state and local entities knowledgeable about K-12 cybersecurity, eight reported having no reporting requirements for cyber incidents and five reported having voluntary reporting mechanisms.[34] For example, officials from Pennsylvania, Connecticut, and Texas reported having varying reporting requirements. Further, Pennsylvania officials said the state has no reporting requirements but allows for school districts to voluntarily report a cybersecurity incident to the state's reporting system. Officials from Connecticut said the state

[34]Some organization officials did not comment on reporting requirements in their state.

GAO-23-105480 K-12 Cybersecurity Coordination

does not have mandatory reporting requirements for school districts, but school districts can voluntarily report a cybersecurity incident to the FBI, DHS, or fusion centers.[35]

Furthermore, Texas officials said that while the state requires school districts to report data breach incidents that include the compromise of sensitive student information, reporting of all other cybersecurity incidents is voluntary. The Texas officials said that many school districts only report on data breaches and not on other types of cyber incidents because they fear that they may be targeted by attackers again or because their cybersecurity insurers prohibit the sharing of information regarding a cybersecurity incident.

While most state and local-level officials reported there are no requirements to report cyber incidents not involving breaches of personal information, Michigan officials said that the state enacted new legislation that will require certain schools to provide a report to the department of state police within 24 hours following a cybersecurity incident. While Michigan requires school districts to report incidents, officials said the purpose of this requirement is to allow Michigan to track incidents.

To increase the reporting of cyber-related incidents to the federal government, the *Cyber Incident Reporting for Critical Infrastructure Act of 2022,* enacted on March 15, 2022, as part of the *Consolidated Appropriations Act, 2022*, requires covered entities[36] across critical infrastructure sectors to report "covered incidents" to CISA within 72 hours of reasonably determining a "covered incident" occurred.[37] CISA has 24 months from the date the act was signed into law to issue the proposed rule, and an additional 18 months to finalize it.[38] As of August 2022, CISA had not issued rules for such reporting, but had issued a request for information to receive input on the proposed regulations. We

---

[35]In general, fusion centers provide a mechanism for multiple federal, state, and local entities to collaborate and share resources, expertise, and information. Their goal is to maximize the ability to detect, prevent, investigate, and respond to all hazards, including criminal or terrorist threats. See 6 U.S.C. § 124h(k)(1).

[36]The act defines the term "covered entities" as an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21.

[37]6 U.S.C. § 681b(a)(1)(A).

[38]6 U.S.C. § 681b(b)(1),(2).

will continue to monitor CISA's progress in developing the incident reporting rules.

Limited Federal and K-12 Schools' Cybersecurity Coordination Increases Challenges' Impact

The fiscal year 2021 NDAA establishes roles and responsibilities for SRMAs to, among other things, coordinate with DHS, regulatory agencies, and others.[39] In addition, the National Plan sets up a framework for sharing information across and between federal and nonfederal stakeholders within each sector that includes the establishment of coordinating councils. Government coordinating councils are to be comprised of representatives from federal, state, local, tribal, and territorial government entities for each sector.

The government coordinating councils enable interagency, intergovernmental, and cross-jurisdictional coordination within and across sectors. In addition, the National Plan states that the critical infrastructure community is to assess their effectiveness by developing metrics to support national goals and priorities as well as sector-specific priorities.

Officials from entities knowledgeable about K-12 cybersecurity reported experiencing limited to no interactions between their districts and federal agencies regarding cybersecurity-related assistance to the K-12 community. This is due in part to Education not establishing a government coordinating council within the Education Facilities Subsector.

Such a council can allow federal agencies to coordinate with each other or with K-12 schools to address schools' cybersecurity risks or to enhance awareness of available federal cybersecurity support. Additionally, although Education and CISA have available resources for the K-12 community, neither agency measures the effectiveness of their cybersecurity-related services or the community's use of them.

---

[39]The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Fiscal Year 2021 NDAA), Pub. L. No. 116-283, § 9002, 134 Stat. 4768 (Jan. 1, 2021).

Officials from entities knowledgeable about K-12 cybersecurity also identified challenges they face to protect and respond to cyber threats and opportunities for federal agencies to possibly better assist them in protecting and responding to cyberattacks in the future.

Without establishing a council for communication and coordination with the K-12 community and metrics to measure the effectiveness of federal support, agencies will be less likely to meet the needs of the subsector and ensure that schools have adequate support to combat evolving cybersecurity threats. In addition, agencies will be less likely to be aware of and develop ways to assist the K-12 community in addressing identified challenges.

Lack of a Coordinating Mechanism Limits Federal Coordination among Agencies and with the K-12 Community

The National Plan calls for the development of government coordinating councils to create an organization for government entities to work together to, among other things, address a respective sector's need for federal assistance. Government coordinating councils enable interagency, intergovernmental, and cross-jurisdictional coordination within and across sectors.

Federal agencies conduct some limited coordination with each other regarding cybersecurity at K-12 schools. More specifically,

- Education coordinates broadly with the FBI on an as-needed basis to discuss specific threats and information the FBI deems to be of concern regarding the Education Subsector. For example, Education officials said that they coordinated with the FBI to issue a public service announcement regarding cyber threat actors.[40] In April 2022, Education officials said that to improve its coordination efforts, they were working to hire a dedicated full-time employee in OSSS who would lead and coordinate OSSS efforts and be responsible for coordinating cybersecurity activities with CISA. They plan to fill this position in fiscal year 2023.

- CISA also collaborates with Education's OSSS to (1) develop federal resources to help K-12 schools combat cyber threats and support

[40]Education's Privacy Technical Assistance Center issued a cyber advisory regarding the specific cyber threat actors.

engagement of school practitioners and (2) perform outreach to schools. For example, according to CISA officials, they worked closely with Education to create fact sheets that identify and develop achievable metrics for the sector and Education.

- FCC officials said that, as of fall 2021, they were in discussions with CISA to create a portfolio of CISA cybersecurity resources that the FCC could direct school districts to use to address their cybersecurity risks. FCC officials indicated in July 2022 that they were initiating coordination with Education, the FBI and other independent and executive branch regulators regarding the E-rate program.

In addition to coordinating among each other, federal agencies conduct some limited coordination with the Education Subsector to address cybersecurity risks. For example,

- CISA is taking steps to coordinate with organizations that advocate for the K-12 community. For example, CISA officials said that their agency regularly engages with a K-12 nonprofit, the Consortium for School Networking, which acts as the conduit for sharing information to its member school districts.[41]

- According to CISA officials, much of its coordination efforts with the K-12 community is done through the MS-ISAC. Officials from school districts and organizations that provide support to K-12 schools reported receiving incident support from CISA. Specifically, officials from seven of 18 school district and state-level organizations said that they received support from the MS-ISAC. Officials from three of the seven school districts said that CISA provided products and threat intelligence, and one said they received incident response assistance. Also, an official from one school district said that CISA provided preventative and diagnostic measures, and phishing training exercises.

- FBI officials stated the FBI field offices are responsible for investigating crimes associated with cyber-related incidents at schools, when reported or discovered through the course of other investigations. For example, according to one official from a large school district, while the FBI field office did not directly support their recovery from the incident, the school district provided the FBI field

---

[41]The Consortium for School Networking is a membership organization designed to meet the needs of K-12 education technology leaders. It supports the entire IT team in a school system/district and offers members the opportunity to meet and communicate with their peers and leaders in the field and participate in local chapters.

office a copy of its incident report and a copy of the school district's hard drive image so the FBI could further investigate the incident.[42]

- The FCC's E-rate program provides funding for K-12 schools to pay for basic internet firewall services. For example, officials from two of seven school districts and one state-level IT and cybersecurity organization noted that they use the FCC's E-rate program to acquire funding for basic internet firewall services.

While this limited coordination occurs, Education has not yet established a government coordinating council within the Education Facilities Subsector to address cybersecurity in the subsector. In addition, none of the officials from 18 state and local entities knowledgeable about K-12 cybersecurity said they had received any type of support from Education, the SRMA for the Education Facilities Subsector. See appendix III for a detailed summary on the views of selected school districts and organizations regarding the limited to no incident support received from Education, CISA, the FBI, and the FCC.

According to Education officials, the department has not yet established a formal mechanism for coordinating within the subsector because it is unsure that it has the necessary authority to do so. Education officials stated that their authority is limited to privacy, which, according to them, limits their ability to act as the lead coordinator for the Education Subsector in terms of providing information security guidance. However, as the SRMA for the Education Facilities Subsector, Education is tasked with coordinating and collaborating with federal and nonfederal entities to support the subsector. As such, we continue to believe that Education's role for coordinating with the K-12 community does not require the department to take unauthorized actions to fulfill their responsibilities as SRMA for the subsector.

By not establishing a coordinating council for the Education Facilities Subsector, Education lacks the involvement of representatives from all levels of government to promote coordination and information-sharing activities required to implement and sustain the subsector's critical infrastructure protection efforts. Without adequate interagency coordination and federal coordination with K-12 schools, agencies are less likely to build relationships within the K-12 community that would

---

[42]Imaging a hard drive is often used to assist law enforcement with reconstructing events, and to determine the "who, what, where, when, and how" of a cyber-related incident.

enable them to assist schools better protect against evolving cyber threats.

Education and CISA Have Not Assessed the Effectiveness of Cybersecurity Resources Available to the Education Subsector

The 2013 National Plan states that the critical infrastructure community is to assess their effectiveness. To measure effectiveness, the National Plan states that agencies are to develop metrics to support national goals and priorities as well as sector-specific priorities. In addition, the National Plan states that owners and operators can support improvements by providing ongoing feedback on the needs and the application of information products by sharing information with the federal government. While Education and CISA have federal resources that are available for K-12 schools to enhance cybersecurity, they have not developed metrics for assessing the effectiveness of these actions. Methods of assessment could include developing and implementing metrics and analyzing feedback from the subsector provided through a government coordinating council regarding the usefulness of federal support.

Education Has No Government Coordinating Council to Obtain Feedback from Schools and No Metrics to Determine Resource Effectiveness

Education has no government coordinating council in place for schools to provide feedback. In addition, officials from Education's OSSS said that they do not have methods to measure the effectiveness of the cybersecurity-related resources and support offered through their websites.

Education officials also said that they do not collect information or conduct targeted research on how information is disseminated to school districts from their technical assistance centers. We previously reported that Education's technical assistance centers were established to share numerous tools, guidance, and online safety resources for K-12 schools and institutions of higher education.[43]

Education officials stated that they do not have the authority to enforce the use of the department's products and services or to require

---

[43]GAO-22-105024.

information on the products' and services' effectiveness. The officials also believe that providing products and services does not necessarily equate to improved cybersecurity for the subsector.

Although Education cannot compel participation from the K-12 community, based on the views we obtained from selected school districts and organizations, it is clear that the K-12 community would more likely use the services and report on the services effectiveness if they were aware of them.

For example, officials from 11 of 18 entities stated that federal agencies could provide more K-12 school specific guidance regarding cybersecurity. Another official stated that the federal government should enhance awareness of products and services as it could help school districts plan their cybersecurity activities around those products and services. We report more details on these opportunities identified by state and local-level officials further in this report.

Due to its concern about its authority to act, Education has only started to take actions related to its SRMA role. As such, in the absence of an Education Facilities Subsector government coordinating council, there is no mechanism for K-12 stakeholders to provide feedback regarding the products and services that are available to them. Without feedback and effectiveness measures, Education may be less likely to meet the needs of the subsector to protect and defend against cyber threats.

CISA Provides Cybersecurity Services but Does Not Measure Their Effectiveness

Although CISA provides a variety of cybersecurity products and services that are available to K-12 school districts, it has no mechanisms in place to measure the effectiveness of those resources. According to an official from CISA's Cybersecurity Division, CISA does not have any mechanisms in place to measure the effectiveness of cybersecurity resources they offer to schools. Further, with no government coordinating council for the Education Facilities Subsector, there is currently no formal mechanism for schools to provide ongoing feedback to CISA. The official said that K-12 schools can provide feedback through the MS-ISAC's national cyber report, which includes measurements in cybersecurity

areas compared to the NIST cybersecurity framework, however such feedback is voluntary.[44]

Without assessing the effectiveness of its federal resources that are available to the Education Subsector, Education and CISA will be less likely to identify gaps in their resources or assist K-12 school districts in enhancing their cybersecurity based on needs. In addition, they will be less likely to understand the effectiveness of their actions.

K-12 School Districts Reported Challenges and Opportunities for Addressing Cybersecurity Threats

Officials from selected entities that are knowledgeable about K-12 cybersecurity stated that K-12 school districts face a variety of challenges to protect their schools from, and to be able to respond to, cyber threats. Those challenges include having a lack of resources and staff, implementing cybersecurity controls and practices, and communicating the cybersecurity risks to leadership at school districts. In addition, these officials identified various opportunities for the federal government that could possibly better assist K-12 school districts in regards to cybersecurity. Those opportunities include providing further funding, training, and resources, as well as more incident response support, and enhancing awareness of school cybersecurity issues and coordination with K-12 schools.

While Federal Agencies Offer Products and Services, K-12 Community Reported Challenges in Mitigating Cyber Threats

School districts and the IT and cybersecurity organizations that support them reported facing various challenges to protect and respond to cyber threats at K-12 schools. These challenges to addressing cyber-related threats are summarized in table 2. More detailed information about each identified challenge follows the table.

---

[44]National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Washington, D.C.: April 16, 2018).

Table 2: Cybersecurity-Related Challenges Identified by Officials at School Districts and State-Level IT and Cybersecurity Organizations

Type of cybersecurity challenge	Number of entities experiencing the challenge
Limited funding	11 of 18
Inadequate staffing	10 of 18
Difficulty maintaining hardware and software upgrades	7 of 18
Lack of end-user education on cyber threats	6 of 18
Low prioritization by school district leaders about cyber threats	5 of 18
Inadequate cybersecurity-related policies and procedures	4 of 18
Difficulty acquiring and maintaining cyber insurance	4 of 18

Source: GAO analysis of school districts and IT and cybersecurity organization interviews. | GAO-23-105480

- **Limited funding:** Officials from 11 of 18 entities stated that there is limited funding for cybersecurity at school districts. For example, an official from a Pennsylvania state-level organization stated that school districts in his purview lacked the funds for cybersecurity defense. In addition, research from a Carnegie Mellon Institute for Critical Infrastructure Technology joint study found that K-12 schools' budgets have struggled to meet cybersecurity needs.[45]

- **Inadequate staffing:** Officials from 10 of 18 entities stated that they lacked enough cybersecurity staff. For example, officials from one California school district stated that they lack enough cybersecurity staff because they cannot meet salary demands. They added that this caused one position to be unfilled for over a year. Further, officials from six of 18 entities stated that their staff lacked technical cybersecurity expertise. Research from Carnegie Mellon found that there is a lack of expertise at K-12 schools, which sometimes only have one or two staff members managing their networks and IT infrastructure.[46]

[45]Mack Peterman, Regan McGovern, Jordan Christian, Lexi Rutkowski, and Saurabh Pethe, with the Carnegie Mellon Institute for Critical Infrastructure Technology, *The State of Cybersecurity in K-12 and Higher Education: Risk Assessment and Analysis* (Pittsburgh, PA: 2022), accessed May 18, 2022, https://icitech.org/cybersecurity-education/.

[46]Mack Peterman, Regan McGovern, Jordan Christian, Lexi Rutkowski, and Saurabh Pethe, *The State of Cybersecurity in K-12 and Higher Education*, 2022.

- **Difficulty maintaining hardware and software upgrades:** Officials from seven of 18 entities also noted difficulty maintaining hardware and software upgrades. For example, a Pennsylvania state-level IT and cybersecurity organization stated that cybersecurity vulnerabilities appear so quickly that it makes it difficult for school districts to mitigate them. The official also reported that many school districts have a large number of connected devices, which make patch management difficult.

- **Lack of end-user education on cyber threats:** Officials from six of 18 entities noted that they lacked enough end-user education regarding cybersecurity threats. For example, an official from a Connecticut state-level IT and cybersecurity organization stated that end-user training is particularly important because it would significantly decrease the number of successful cyber-attacks at K-12 school districts.

- **Low prioritization by school district leaders:** Officials from five of 18 entities stated that school district leaders do not prioritize cybersecurity highly enough. For example, officials from one California school district stated that school district leaders do not allocate enough staff or funding to cybersecurity areas because they do not see it as a threat.

- **Inadequate cybersecurity-related policies and procedures:** Officials from four of 18 entities noted that they have inadequate cybersecurity-related policies and procedures. For example, an official from a state association in Texas stated that the school districts in the association's purview are not prepared to handle cybersecurity incidents because the school districts' policies are not sufficient to handle serious cyber threats. In addition, an official from a Pennsylvania state-level organization stated that school districts in his purview that experienced ransomware attacks were not prepared because they had no policies or procedures in place.

- **Difficulty acquiring and maintaining cyber insurance:** Officials from four of 18 entities stated that it is becoming more challenging for school districts to acquire cybersecurity insurance. According to officials from one school district and two state-level organizations, the difficulty is due to insurance companies' requiring school districts to implement specific cybersecurity practices and cybersecurity controls to be eligible for coverage. For example, officials stated that cybersecurity insurance companies are now requiring multi-factor authentication and user awareness training. These officials also said that some small school districts are not capable or equipped to enable such requirements.

In addition, officials from one school district and four IT organizations that provide support to K-12 school districts stated that their schools' coverage had decreased or ceased due to the insurance companies' perception that the sector's risk is too great. Also, officials from a California organization stated that their cybersecurity insurance premium increased 400 percent in 1 year even though they maintained a clean record with no reported incidents.

Officials further said that most large school districts can afford cyber insurance to respond to a cyber incident, whereas smaller school districts cannot afford the insurance. We reported in June 2022 that federal agencies, including the Department of the Treasury's Federal Insurance Office and CISA, had taken steps to understand the financial implications of growing cybersecurity risks.
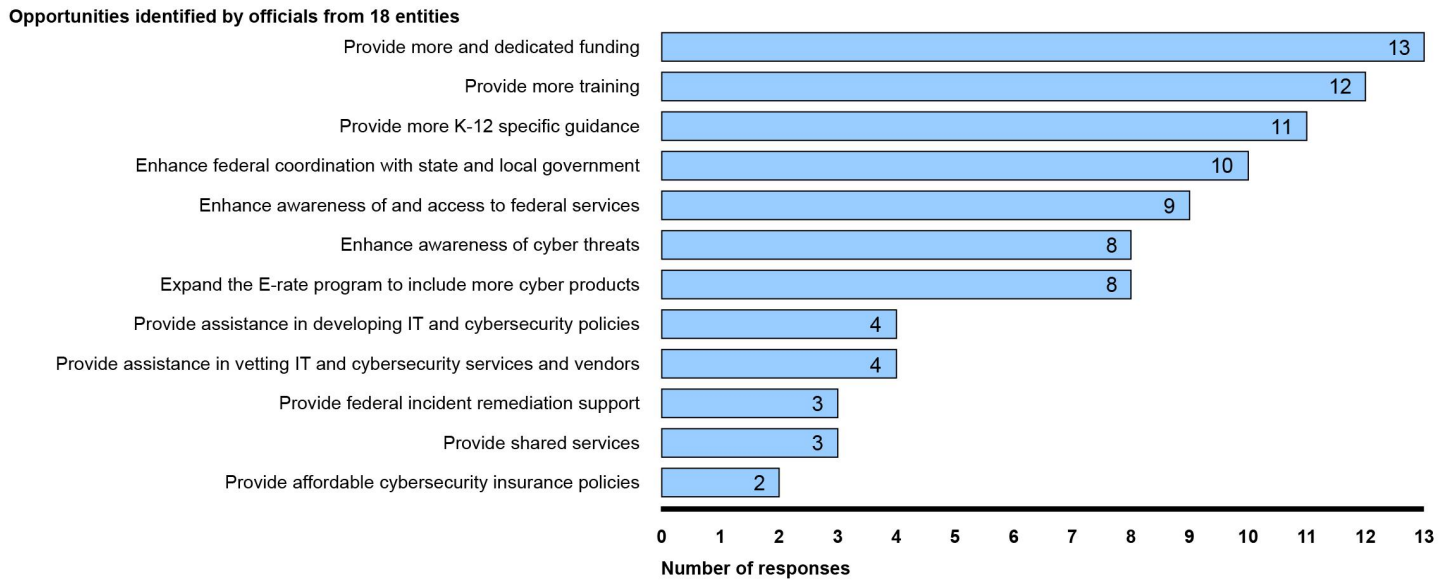
However, they had not assessed the extent to which risks to critical infrastructure from catastrophic cyber incidents and potential financial exposures warranted a federal insurance response.[47] We recommended that the two agencies jointly assess the extent to which risks to critical infrastructure from catastrophic cyber incidents and potential financial exposures warrant a federal insurance response, and inform Congress of the results of their assessment. Both agencies agreed with the recommendations.

K-12 Community Identified Opportunities for Improving Federal Cybersecurity-Related Assistance and Coordination

Officials from K-12 school districts and state and local organizations related to K-12 schools provided their views on the additional federal support that Education, CISA, the FBI, and the FCC could provide to further assist K-12 school districts to address their ongoing cybersecurity challenges. Specifically, officials noted that federal entities could provide or enhance a number of products and services to improve schools' cybersecurity. These opportunities are summarized in figure 5 and discussed in the bulleted list that follows it.

---

[47]GAO, *Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks,* GAO-22-104256 (Washington, D.C.: June 21, 2022).

Figure 5: Possible Opportunities for Federal Agencies to Better Support Schools' Cybersecurity, Identified by K-12 Officials

Opportunities identified by officials from 18 entities

Opportunity	Number of responses
Provide more and dedicated funding	13
Provide more training	12
Provide more K-12 specific guidance	11
Enhance federal coordination with state and local government	10
Enhance awareness of and access to federal services	9
Enhance awareness of cyber threats	8
Expand the E-rate program to include more cyber products	8
Provide assistance in developing IT and cybersecurity policies	4
Provide assistance in vetting IT and cybersecurity services and vendors	4
Provide federal incident remediation support	3
Provide shared services	3
Provide affordable cybersecurity insurance policies	2

Number of responses

Source: GAO analysis of K-12 school district and state and local organizations' interview responses. | GAO-23-105480

Note: The E-rate program is administered by the Federal Communications Commission and provides funding to K-12 schools to acquire telecommunications services, telecommunications, internet access, internal connections, basic maintenance, and managed internal broadband services. The program can cover the cost of certain cybersecurity services such as basic firewall protection through the school's internet service provider.

- **More and dedicated funding:** Officials from 13 of 18 entities stated that federal entities could provide more and dedicated funding to school districts for cybersecurity. For example, officials from two school districts in California and Connecticut stated that they do not have dedicated funding in their district's budget for cybersecurity. The official from California said that not having dedicated funding makes it difficult to acquire cybersecurity-related products. In addition, officials from one Connecticut school district recommended that the federal government provide funding to K-12 school districts to purchase cybersecurity products and services that are needed to secure their networks.

- **More cybersecurity-related training:** Officials from 12 of 18 entities stated that federal entities could provide more cybersecurity training to K-12 school staff. For example, officials from a California school district said the district needed additional training for teachers so teachers can understand how to maintain security, keep their credentials safe, and keep secure the sensitive data that they access. Further, a Pennsylvania school district said that having access to reasonably priced training would help them to enhance their staff's

cybersecurity expertise. This training could include low-cost training through a centralized federal campaign.

- **K-12 specific guidance:** Officials from 11 of 18 entities stated that federal entities could provide more K-12 school-specific guidance regarding cybersecurity. For example, officials from a Connecticut school district stated that the NIST cybersecurity framework is helpful but they would like the federal government to consider creating a K-12 specific set of cybersecurity controls and guidance for the Education Facilities Subsector. We previously recommended that Education determine whether sector-specific guidance is needed for the subsector.[48] As of April 2022, the department reported it plans to identify any gaps within its K-12 products and resources and then meet with CISA to determine whether additional guidance is needed for the subsector.

- **Federal coordination with state and local government:** Officials from 10 of 18 entities knowledgeable about K-12 cybersecurity believe federal entities could enhance their coordination effort with local governments, including K-12 school districts. For example, one California official stated that information and coordination does not always follow through from the federal level to the school district. They added that the federal government should ensure that their efforts make it to local governments.

- **Awareness and access to federal services:** Officials from nine of 18 entities stated that federal agencies could enhance K-12 schools' awareness of the services available to schools to enhance cybersecurity. For example, an official from a Pennsylvania state-level IT and cybersecurity organization stated that the federal government should provide an annual update on the products and services provided to the sector. The official added that this could help school districts to plan their cybersecurity activities around those products and services. Further, one official from a Texas association stated that the federal government should leverage associations and state-level organizations to spread awareness of their products and services.

- **Awareness of cyber threats:** Officials from eight of 18 entities stated that federal entities could work to enhance K-12 schools' awareness of the cyber threats they face. For example, officials from one Pennsylvania IT and cybersecurity organization noted that the federal government could help in spreading awareness of the vulnerabilities and threats facing their networks, software, and devices.

---

[48]GAO-22-105024.

- **E-rate program:** Officials from eight of 18 entities noted that the FCC could expand the E-rate program to include further cybersecurity-related products and services. For example, officials from one California school district stated the FCC should consider including advanced firewall products and the subscriptions that go with the firewall products covered by E-rate because the accompanying subscriptions are crucial to the function of the product and help to ensure the firewalls are kept up to date.

FCC officials noted that the cost of covering advanced cybersecurity services for school districts would likely exceed the funding allocation for the whole program. Specifically, a report from the Consortium for School Networking found that it would cost the E-rate program $2.389 billion annually to provide all K-12 schools with funding for advanced security services.[49] In contrast, according to FCC officials, the estimated funding allocation for the E-rate program for fiscal year 2022 is $3.15 billion to cover all eligible telecommunications services under the program and would likely not be sufficient to cover the cost of advanced security services.

FCC officials said that they received comments from the public and stakeholders as part of the funding year 2022 eligible services list proceeding requesting to add advanced cybersecurity services to the E-rate program. Many stakeholders who sent in comments requested that advanced cybersecurity services be added to the E-rate program. However, the officials said that the Commission declined to expand funding for advanced cybersecurity services as part of the funding year 2022 eligible services list before the pending release of more information from CISA. The officials said that the FCC plans to review the reports produced by CISA as part of the *Cybersecurity Act of 2021* and expressed that this legislation and forthcoming report would provide valuable insight on the cybersecurity services that would be most impactful for K-12 schools.

- **Assistance developing IT and cybersecurity policies:** Officials from four of 18 entities stated that federal entities could provide assistance to K-12 school districts to help develop IT and cybersecurity-related policies.

- **Assistance vetting IT and cybersecurity services and vendors:** Officials from four of 18 entities stated that federal entities could provide vetting of IT and cybersecurity vendors and services. For example, officials from one Texas association said that it would be

---

[49]Consortium for School Networking and Funds for Learning, *E-rate Cybersecurity Cost Estimate* (January 2021).

beneficial if the federal government would provide assistance in vetting software purchases at K-12 schools to help them ensure they are choosing a product with good security.

- **Federal incident remediation support:** Officials from three of 18 entities stated that federal entities could provide school districts with federal incident remediation support. For example, officials from a Pennsylvania state-level IT and cybersecurity organization stated that the federal government should provide more actionable guidance for schools following a cybersecurity incident.

- **Shared services:** Officials from three of 18 entities stated that federal entities could provide shared IT and cybersecurity services to schools. For example, officials from one California school district stated that a federal cyber-related security operations center would help school districts to manage cyber threats to their networks.

- **Affordable cybersecurity insurance policies:** Officials from two entities stated that federal entities could provide schools with more affordable cybersecurity insurance policies due to the rising prices and decreasing coverage provided by insurance companies. As previously mentioned, in June 2022 we made recommendations for CISA and Treasury's Federal Insurance Office to consider federally supported cyber insurance based on the assessment of risks to critical infrastructure from cyber incidents.[50]

The challenges and opportunities identified by officials knowledgeable about K-12 cybersecurity represent items that potentially require greater attention by the community. Although federal agencies are taking steps to help the Education Subsector, these agencies may be able to better enhance school cybersecurity by addressing the challenges and considering the opportunities identified.

Conclusions

K-12 school districts face a broad range of cyber threats. Successful attacks on schools have resulted in monetary and learning loss. While some states have requirements to centrally report cyber-related incidents, the precise national magnitude of the impact of cyber incidents on K-12 schools is unknown due in part to limited reporting requirements.

---

[50]GAO-22-104256.

To address these threats, Education, CISA, and other federal agencies are tasked with providing cybersecurity-related assistance to school districts. However, without a government coordinating council, it is difficult for federal agencies and the K-12 community to coordinate and determine how best to address cybersecurity threats, mitigate the challenges identified, or determine the federal agencies' ability to provide for the opportunities that K-12 officials believe would assist K-12 schools.

Additionally, without measuring the effectiveness of federal support, agencies remain unaware whether schools have adequate resources needed to address cybersecurity threats. As a result, the K-12 community may be insufficiently equipped to protect and defend against growing cyber threats, thus impacting schools' ability to adequately educate students and protect staff and students' information.

Recommendations for Executive Action

We are making four recommendations, three to the Secretary of Education and one to the Secretary of the Department of Homeland Security:

- The Secretary of Education, in consultation with the Cybersecurity and Infrastructure Security Agency and other stakeholders involved in updating the Education Facilities Sector-Specific Plan, should establish a collaborative mechanism, such as an applicable government coordinating council, to coordinate cybersecurity efforts between agencies and with the K-12 community. (Recommendation 1)

- The Secretary of Education should develop metrics for obtaining feedback to measure the effectiveness of Education's K-12 cybersecurity-related products and services that are available for school districts. (Recommendation 2)

- The Secretary of Education, in coordination with federal and nonfederal stakeholders, should determine how best to help school districts overcome the identified challenges and consider the identified opportunities for addressing cyber threats, as appropriate. (Recommendation 3)

- The Secretary of the Department of Homeland Security should ensure that the Director of the Cybersecurity and Infrastructure Security Agency develops metrics for measuring the effectiveness of its K-12 cybersecurity-related products and services that are available for

school districts and determine the extent that CISA meets the needs of state and local-level school districts to combat cybersecurity threats. (Recommendation 4)

Agency Comments and Our Evaluation

We provided a draft of this report to Education, DHS, the FBI, and the FCC for review and comment. In its comments, reproduced in appendix IV, Education concurred with one recommendation and concurred in part with two recommendations. In its comments, reproduced in appendix V, DHS concurred with its one recommendation. Further, we received written technical comments on the draft from DHS's CISA, the FBI, and the FCC, which we have incorporated in the report, as appropriate.

Regarding Education, it concurred with our recommendation to determine how best to help school districts overcome the identified challenges and consider the identified opportunities. The department stated that it has formed an intra-agency coordination working group, participates in informal and formal federal interagency coordination to provide resources to help school districts, and has developed a webpage that includes resources for school districts, parents, and other stakeholders. As previously noted, establishing a formal coordinating mechanism will allow for greater communication with school districts so that Education can obtain feedback regarding the challenges and opportunities identified.
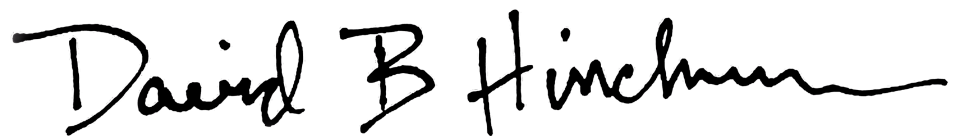
Education concurred in part with the recommendation to establish a collaborative mechanism. Education stated that it already initiated informal interagency coordination with other federal partners and will consider the use of other collaborative mechanisms. Although this informal coordination is a step in the right direction, we continue to believe that establishing a formal coordinating mechanism will allow for greater representation from the K-12 community and all levels of government so that Education can better assist K-12 schools.

Education also concurred in part with the recommendation to establish metrics to measure the effectiveness of its K-12 cybersecurity-related resources. Specifically, the department stated that it agreed to explore what metrics may be useful for obtaining feedback to measure the effectiveness of the department's K-12 cybersecurity-related products and services. If the department establishes effectiveness metrics, Education will be more likely to meet the needs of the subsector to protect and defend against cyber threats.

Finally, DHS concurred with its recommendation and stated that CISA agrees metrics are necessary to measure the effectiveness of CISA's K-12 cybersecurity-related products and services. In addition, CISA stated that it plans to develop the metrics in an effort to determine whether its products and services meet the needs of state and local-level school districts and reported an estimated completion date of October 31, 2023. If CISA establishes effectiveness metrics, the agency will be more likely to identify cybersecurity needs of the subsector to protect and defend against cyber threats.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until four days from the report date. At that time, we will send copies to the appropriate congressional committees, the Secretary of Education, the Secretary of Homeland Security, the Attorney General of the United States, and the Chairwoman of the Federal Communications Commission. In addition, the report will be available at no charge on the GAO website at https://www.gao.gov.

If you or your staff members have any questions about this report, please contact David B. Hinchman at (214) 777-5719 or hinchmand@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix VI.

David B. Hinchman
Acting Director, Information Technology and Cybersecurity

List of Requesters

The Honorable Margaret Wood Hassan
Chair
Subcommittee on Emerging Threats and Spending Oversight
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Kyrsten Sinema
Chair
Subcommittee on Government Operations and Border Management
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Jacky Rosen
United States Senate

The Honorable Chris Van Hollen
United States Senate

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) determine what is known about the cost impact of cyber incidents on school districts and (2) determine the extent to which key federal agencies coordinate with other federal and nonfederal entities to help K-12 schools combat cyber threats.

To address our first objective, we collected and analyzed unpublished K-12 SIX data regarding publicly reported significant K-12 cyber incidents from January 2018 to December 2021. We also collected and analyzed data from the Department of Education's (Education) Common Core of Data regarding the total number of students within each state during the 2019-2020 school year.[1]

We analyzed the data to determine how many incidents occurred in each state during that time frame and organized the states by the most reported state-wide cyber incidents to the least. We then selected three states by identifying the top 10 states that had the most reported K-12 cyber incidents. From those top 10 states, we selected three states based on population, selecting the most and least populated, and one state from the middle range of the group to include California, Pennsylvania, and North Carolina.

In addition, based on referrals from those states, we interviewed officials from Connecticut, Texas, and Michigan because of their reported knowledge about K-12 cybersecurity. We then selected entities from K-12 school districts and state-level organizations, such as state IT and cybersecurity organizations to take part in semi-structured interviews.

To select school districts within each of these selected states, we analyzed the K12 SIX data regarding K-12 cyber incidents and Education's Common Core of Data regarding student population within each school district during the 2019-2020 school year. We included school districts that had experienced at least one cyber incident and

---

[1]K12 SIX is a national nonprofit information sharing organization that assists its members from the K-12 community in protecting them from cybersecurity threats. School districts are not required to report their incidents to K12 SIX, thus the incident data represent a portion of the actual total.

ranked those school districts based on student population according to
Education's data. We then selected and contacted three school districts in
each state of California, Pennsylvania, and North Carolina. We
determined the school districts to contact based on student population. Of
those contacted, officials from seven school districts agreed to participate
in our study.

In total, we interviewed officials from 18 state and local entities from the
six selected states. The officials were responsible for or knowledgeable
about K-12 cybersecurity within the K-12 community and represented
seven school districts, 10 IT and cybersecurity organizations, and one
association. Specifically, officials were from California (three school
districts[2] and three IT and cybersecurity organizations); Pennsylvania
(one school district[3] and two IT and cybersecurity organizations); North
Carolina (one school district and two IT and cybersecurity organizations);
Connecticut (two school districts and one IT and cybersecurity
organization); Texas (one association and one IT and cybersecurity
organization); and Michigan (one IT and cybersecurity organization).

We collected and analyzed available evidence and interviewed these
officials from the selected school districts, IT and cybersecurity
organizations, and an association in those states to obtain their views on
the impact of cyber incidents. We analyzed these interviews by
developing and sorting interview responses into categories.

We then calculated the total number of responses in each category to
identify trends in responses regarding federal coordination efforts to
assist school districts, the impact of cyber incidents on school districts,
challenges to protect from and respond to cyber incidents, and views on
how the federal government can better assist schools.

In addition, we collected and analyzed data from relevant reports and
studies about cybersecurity incidents at K-12 schools and the impact of
those incidents, including public and nonpublic data from Comparitech
regarding the impact of ransomware incidents at K-12 school districts
from January 2018 to December 2021. We analyzed the data to identify

---

[2]Out of the three school districts in California, one was not part of our selection but
volunteered to take part in our review.

[3]The Pennsylvania school district was not part of our selection but volunteered to take part
in our review.

trends in the total downtime and cost of downtime from ransomware attacks.

We assessed the quality and reliability of the data by interviewing an official from Comparitech regarding the company's methodology for the study, including the sources used to collect the data and steps taken to ensure the data were entered accurately. We found that the publicly and non-publicly reported data based on information Comparitech collected were reliable for the purpose of summarizing results as background to provide context for our findings.

To address our second objective, we examined relevant law and federal guidance, such as the *National Defense Authorization Act (NDAA) for Fiscal Year 2021* and the *National Infrastructure Protection Plan* (National Plan).[4] Based on our analysis, we identified key federal agencies that support the Education Subsector including Education, the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Bureau of Investigation (FBI). In addition, we identified the Federal Communications Commission (FCC) as a key agency for supporting the subsector through its E-rate program.[5]

We then identified key laws and federal guidance that specify federal agency responsibilities for coordinating with each other and with nonfederal entities to provide assistance to school districts. These authorities include: the NDAA for fiscal year 2021; the *Telecommunications Act of 1996; the K-12 Cybersecurity Act of 2021;* Executive Order 13636*: Improving Critical Infrastructure Cybersecurity*; Presidential Policy Directive 41: *United States Cyber Incident Coordination;* Presidential Decision Directive 63: *Protecting America's Critical Infrastructures,* National Institute of Standards and Technology's

---

[4]*The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021* (Fiscal Year 2021 NDAA), Pub. L. No. 116-283, § 9002; Department of Homeland Security, *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: December 2013).

[5]The FCC oversees the E-rate program, which provides funding to K-12 schools to acquire telecommunications services, telecommunications, internet access, internal connections, basic maintenance, and managed internal broadband services. The program can cover the cost of certain cybersecurity services such as basic firewall protection through the school's internet service provider.

(NIST) *Framework for Improving Critical Infrastructure Cybersecurity*, and
the National Plan.[6]

We also collected and analyzed relevant documents and interviewed
officials from Education, CISA, the FBI, and the FCC about the actions
taken to coordinate with each other and with other federal agencies and
nonfederal entities to enhance awareness of federal support to assist K-
12 school districts to protect and defend against cyber threats, and
respond to cyber incidents. We then compared these agencies'
coordination efforts to provide assistance to K-12 school districts to
coordination requirements set forth in applicable law and federal
guidance, such as the fiscal year 2021 NDAA and the National Plan, to
determine whether they met requirements.

We obtained testimonial evidence regarding actions taken by the federal
government to provide assistance to K-12 school districts and the level of
federal coordination efforts between these entities to improve
cybersecurity for K-12 schools. We analyzed these interviews by
developing and sorting interview responses into categories. We then
calculated the total number of responses in each category to identify
reported trends regarding federal coordination efforts with K-12 school
districts and state-level organizations, the extent officials were aware of
and made use of federal support, and views on how the federal
government can better assist K-12 schools to address cybersecurity.

We conducted this performance audit from October 2021 to October 2022
in accordance with generally accepted government auditing standards.
Those standards require that we plan and perform the audit to obtain
sufficient, appropriate evidence to provide a reasonable basis for our
findings and conclusions based on our audit objectives. We believe that
the evidence obtained provides a reasonable basis for our findings and
conclusions based on our audit objectives.

---

[6]*Telecommunications Act of 1996*, Pub. L. No. 104-104, 110 Stat. 56, (1996); *The K-12
Cybersecurity Act of 2021*, Pub. L. No. 117-47, 135 Stat. 397, 397-98 (2021); The White
House, *Improving Critical Infrastructure Cybersecurity*, Executive Order 13636
(Washington, D.C.: Feb. 12, 2013); The White House, *United States Cyber Incident
Coordination*, Presidential Policy Directive 41 (Washington, D.C.: July 26, 2016); The
White House, *Protecting America's Critical Infrastructures*, Presidential Decision Directive
63 (Washington, D.C.: May 22, 1998); National Institute of Standards and Technology,
Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (Washington,
D.C.: April 16, 2018).

Appendix II: Federal Laws, Policies, and Plans Establish Roles and Responsibilities for K-12 School Cybersecurity

Table 3 identifies federal laws, policies, and public-private plans that establish the roles and responsibilities for the protection of critical infrastructure, including the Education Facilities Subsector.

Table 3: Federal Laws and Public-Private Plans That Pertain to the Education Facilities Subsector

Federal Law, Policy, or Plan	Description
The National Defense Authorization Act for Fiscal Year 2021[a]	Established, among other things, the roles and responsibilities for sector risk management agencies (SRMAs) in supporting the protection of the 16 critical infrastructure sectors. Responsibilities include coordinating and supporting sector risk management efforts; assessing sector risk, in coordination with the Cybersecurity and Infrastructure Security Agency (CISA) and the sector; serving as a day-to-day federal interface for the prioritization and coordination of sector-specific activities; and supporting incident management, including supporting CISA, upon request, in asset response activities.
Telecommunications Act of 1996[b]	Mandated, among other things, that the Federal Communications Commission (FCC) establish the schools and libraries universal service support program, commonly known as the E-rate program. The E-rate program is to ensure that schools and libraries have affordable access to advanced telecommunications and information services to use for educational purposes at discounted rates.
K-12 Cybersecurity Act of 2021[c]	Required CISA to take steps to address cybersecurity at K-12 schools. Specifically, CISA is to: (1) conduct a study of the impact of cybersecurity risks on schools, the challenges of remote learning, and evaluate the most accessible ways to communicate cybersecurity recommendations and tools, and brief Congress on those results; (2) develop voluntary recommendations for addressing cybersecurity risks in schools; and (3) develop an online training toolkit to educate school officials on its recommendations and to provide implementation strategies for those recommendations.
Executive Order 13636*: Improving Critical Infrastructure Cybersecurity*[d]	Issued in 2013, this order called for a partnership with the owners and operators of critical infrastructure to improve cybersecurity-related information sharing. Among other things, the order designated federal sector-specific agencies (called SRMAs per fiscal year 2021 NDAA). The SRMAs serve as the lead agencies for coordinating federally sponsored activities within their sectors. Further, the order directed the Department of Homeland Security (DHS), with help from the SRMAs, to identify and annually review and update a list of critical infrastructures for which a cybersecurity incident could reasonably result in catastrophic effects on public health or safety, economic security, or national security.

Federal Law, Policy, or Plan	Description
Presidential Policy Directive (PPD) 41: *United States Cyber Incident Coordination*[e]	Issued in 2016, PPD-41 sets forth principles governing the federal government's response to any cyber incident, whether involving government or private-sector entities. According to the directive, federal agencies are to undertake three concurrent lines of effort when responding to any cyber incident: threat response; asset response; and intelligence support and related activities.
Presidential Decision Directive 63: *Protecting America's Critical Infrastructures*[f]	Issued in 1998, the directive created the concept of Information Sharing and Analysis Centers (ISACs). ISACs are intended to help critical infrastructure owners and operators protect facilities, personnel, and customers from cyber and physical security threats and other hazards. ISACs are nonprofit, member-driven organizations formed by critical infrastructure owners and operators to share information between government and industry.
National Institute of Standards and Technology: *Framework for Improving Critical Infrastructure Cybersecurity*[g]	Developed in 2014, this voluntary framework of cybersecurity standards and procedures was updated in 2018. Its risk-based approach to managing cybersecurity is composed of three major parts: a framework core, profiles, and implementation tiers. The framework core provides a set of activities to achieve specific cybersecurity outcomes and references examples of guidance to achieve those outcomes. The framework specifies controls that support the core security functions of identifying, protecting, detecting, responding to, and recovering from security incidents.
National Infrastructure Protection Plan[h]	Developed in response to PPD-21[i] by DHS in 2013. The National Plan, intended to serve as a national guide for the management of risks to critical infrastructure, breaks down the policy requirements in Executive Order 13636 and PPD-21 into risk management-related goals and objectives.
Government Facilities Sector-Specific Plan (SSP)[j]	Developed in 2015 by the General Services Administration and DHS to help understand evolving risk to the Government Facilities Sector's assets and functions.
Education Facilities Sector-Specific Plan[k]	Developed in 2010 by Education and DHS, as an annex to the Government Facilities SSP, the plan designates Education as the SRMA for the Education Facilities Subsector. As such, Education is to lead efforts, in collaboration with subsector federal and nonfederal stakeholders, to understand cybersecurity risks facing the subsector and enhance the cybersecurity of the subsector, among other things.

Source: GAO summary of identified federal laws, policies, and plans. | GAO-23-105480

[a]*The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021,* Pub. L. No. 116-283, § 9002 (2021).

[b]*Telecommunications Act of 1996,* Pub. L. No. 104-104, 110 Stat. 56, 72 (1996).

[c]*K-12 Cybersecurity Act of 2021,* Pub. L. No. 117-47, 135 Stat. 397, 397-98 (2021).

[d]The White House, *Improving Critical Infrastructure Cybersecurity,* Executive Order 13636 (Washington, D.C.: Feb. 12, 2013).

[e]The White House, *United States Cyber Incident Coordination,* Presidential Policy Directive 41 (Washington, D.C.: July 26, 2016).

[f]The White House*, Protecting America's Critical Infrastructures,* Presidential Decision Directive 63 (Washington, D.C.: May 22, 1998).

[g]National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity,* Version 1.1 (Washington, D.C.: April 16, 2018).

[h]Department of Homeland Security, *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: December 2013).

[i]The White House, Critical Infrastructure Security and Resilience, Presidential Policy Directive 21 (Washington, D.C.: Feb. 12, 2013).

[j]General Services Administration and Department of Homeland Security, Government Facilities Sector-Specific Plan (2015).

[k]Department of Homeland Security and Department of Education, *Education Facilities Sector-Specific Plan: An Annex to the Government Facilities Sector-Specific Plan* (2010).

Appendix III: K-12 Community Reported Receiving Limited Federal Support

Selected school districts and organizations reported receiving limited or no incident support from the Department of Education, Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Bureau of Investigation (FBI). In addition, school districts reported that the Federal Communications Commission's (FCC) E-rate program provided limited funds to assist them in providing cybersecurity services. These views are discussed in the bulleted list below.

- **Selected School Districts and Organizations Reported Receiving No Cybersecurity Support from Education.** The *National Defense Authorization Act (NDAA) for Fiscal Year 2021* requires sector risk management agencies (SRMA) to serve as a day-to-day federal interface for the prioritization and coordination of sector-specific activities. As the SRMA, Education is to fulfill this role for the Education Subsector. However, none of the officials from 18 state and local entities knowledgeable about K-12 cybersecurity said they had received any type of support from Education. In addition, some school district officials said that they were unclear about who to contact for such support, and further, were unaware of the products and services that Education offers. For example, a chief information officer from Michigan and a chief information security officer from Pennsylvania, who both provide IT support to school districts under their purview, reported it was unclear who they should contact to receive federal support. In another example, a California school district chief technology officer said that the organization had used Education's technical assistance center webpage in the past, but was under the impression it had since closed. However, as of August 2022, the webpage was active.

- **Selected School Districts and Organizations Reported Receiving Limited Incident Support from CISA.** As the lead federal agency for the protection of critical infrastructure, CISA is responsible for providing strategic guidance, promoting a national unity of effort, and coordinating the overall federal effort to promote the security and

resilience of critical infrastructure.[1] One state-level IT organization official said that they requested CISA's penetration testing service and were placed on about a 2-year waiting list. The official expressed that their experience with CISA led them to believe that federal products and services are aimed at other sectors of the critical infrastructure, but not at K-12 schools, and that no one is focusing on K-12 cybersecurity.

According to CISA officials, much of its coordination efforts with the K-12 community is done through the Multi-State Information Sharing and Analysis Center (MS-ISAC). Officials from seven of 18 school district and state-level organizations said that they received support from the MS-ISAC. These services included their guidance and policies; penetration testing; network scanning; and network monitoring tools. In addition, CISA officials said that they created a K-12 resource page, which features consolidated and digestible resources for K-12 schools. However, as we previously reported,[2] many school districts that are not members of the MS-ISAC may not have the opportunity to benefit from the various products and services that it offers.[3]

- **Selected School Districts and Organizations Reported Receiving Limited to No Cybersecurity Incident Support from the FBI.** When incidents are reported, the FBI's field offices handle threat response activities at K-12 schools. Officials from four school districts and three state-level IT and cybersecurity organization stated that they received little to no support from the FBI following a cyber incident. In response to what these state and local-level officials reported, FBI officials stated that, as noted earlier, the bureau's responsibilities are to investigate cyberattacks and seek to identify those responsible. The FBI officials also maintained that their ability to provide support is based upon the circumstances of the incident, such as information that is provided by the victim.

- **FCC's E-Rate Program Provides Limited Funding for Cybersecurity Service.** The FCC officials we interviewed stated that

---

[1]As part of the *K-12 Cybersecurity Act of 2021,* Pub. L. No. 117-47, 135 Stat. 397, 397-98 (2021)*,* CISA is required to conduct a study at K-12 schools and report on how cybersecurity risks impact schools. CISA is further required to develop voluntary recommendations to address those risks and develop a cybersecurity toolkit for K-12 school districts.

[2]GAO-22-105024.

[3]CISA reported that about 3,700 K-12 entities were using the MS-ISAC's services as of September 2022.

the E-rate program includes funding for certain cybersecurity services, such as basic firewall protection included in the Internet access provided by the school district's internet service provider as a Category 1 service, and separately priced components for basic firewall protection as a Category 2 service.[4]

---

[4]According to the FCC, a basic firewall is hardware and software that sits at the boundary between an organization's network and the outside world and protects the network against unauthorized access or intrusions.

Appendix IV: Comments from the Department of Education

UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF ELEMENTARY AND SECONDARY EDUCATION

October 7, 2022

David B. Hinchman, Acting Director
Information Technology and Cybersecurity
Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548
hinchmand@gao.gov

Dear Acting Director Hinchman,

Thank you for the opportunity for the U.S. Department of Education (Department) to provide comments on, and respond to the three recommendations made in, the Government Accountability Office's (GAO) draft report entitled, *Critical Infrastructure Protection: Additional Federal Coordination is Needed to Enhance K-12 Cybersecurity* (GAO-23-105480). As a Deputy Assistant Secretary of the Office of Elementary and Secondary Education (OESE), I am pleased to respond on behalf of the Department.

Given Education's commitment to enhancing K-12 cybersecurity, the Department has engaged in both formal and informal coordination internally and across agencies and strives for continuous improvement (while continuing to take into account the limitations on its authority in this area). For example, when contacted regarding the recent ransomware attack on the Los Angeles Unified School District (LAUSD) last month, the Department leveraged a new intra-agency cybersecurity working group to quickly establish a "Cyberhelp" website highlighting the most impactful cybersecurity resources from across the Department to support school districts and other stakeholders to prepare for and respond to cybersecurity incidents. The Department will soon add one career staff person who will be focused on cybersecurity-related matters through our programs in the Office of Safe and Supporting Schools, and also recently "onboarded" a Digital Infrastructure Fellow in the Office of Educational Technology, to increase its capacity for formal and informal federal, state, and local coordination.

GAO made three recommendations to the Department:

Recommendation 1 - The Secretary of Education, in consultation with the Cybersecurity and Infrastructure Security Agency (CISA) and other stakeholders involved in updating the Education Facilities Sector-Specific Plan, should establish a collaborative mechanism, such as an applicable government coordinating council, to coordinate cybersecurity efforts between agencies and the K-12 community.

ED Response: The Department concurs in part with the recommendation regarding the need for collaboration with other federal partners regarding K-12 cybersecurity. Additionally, the Department has already begun informal interagency coordination with other federal partners and stakeholders, including the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Communications Commission (FCC) and the Office of the National Cyber Director, and is considering the use of other collaborative mechanisms. We will work with the other federal partners and stakeholders to help determine the appropriate mechanisms for further activities.

Recommendation 2 - The Secretary of Education should develop metrics for obtaining feedback to measure the effectiveness of Education's K-12 cybersecurity-related products and services that are available for school districts.

ED Response: The Department concurs in part with this recommendation and agrees to explore whether and what metrics may be useful for obtaining feedback to measure the effectiveness of the Department's K-12 cybersecurity-related products and services that are available for school districts.

Recommendation 3 - The Secretary of Education, in coordination with federal and nonfederal stakeholders, should determine how best to help school districts overcome the identified challenges and consider the identified opportunities for addressing cyberthreats, as appropriate.

ED Response: The Department concurs with this recommendation and has begun the process of identifying ways to assist school districts in overcoming challenges to the extent those challenges are appropriate to the federal role. As noted above, the Department has formed an intra-agency coordination working group and also participates in informal and formal federal interagency coordination to provide resources to help school districts. Towards that end, the Department has already developed a webpage of curated resources, including resources for school districts, parents and other stakeholders at http://tech.ed.gov/cyberhelp. The Department is committed to regularly updating this page as well as identifying and developing additional resources focused on this critical topic.

Thank you for your consideration of the Department's feedback on the three recommendations made in GAO's draft report.

Respectfully,

MARK
WASHINGTON

Digitally signed by MARK
WASHINGTON
Date: 2022.10.07
15:50:29 -04'00'

Mark Washington
Deputy Assistant Secretary
Office of Elementary and Secondary Education

Agency Comment Letter

Text of Appendix IV: Comments from the Department of Education

October 7, 2022

David B. Hinchman, Acting Director
Information Technology and Cybersecurity
Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548
hinchmand@gao.gov

Dear Acting Director Hinchman,

Thank you for the opportunity for the U.S. Department of Education (Department) to
provide comments on, and respond to the three recommendations made in, the
Government Accountability Office's (GAO) draft report entitled, Critical Infrastructure
Protection: Additional Federal Coordination is Needed to Enhance K-12
Cybersecurity (GAO-23-105480). As a Deputy Assistant Secretary of the Office of
Elementary and Secondary aEducation (OESE), I am pleased to respond on behalf
of the Department.

Given Education's commitment to enhancing K-12 cybersecurity, the Department
has engaged in both formal and informal coordination internally and across agencies
and strives for continuous improvement (while continuing to take into account the
limitations on its authority in this area). For example, when contacted regarding the
recent ransomware attack on the Los Angeles Unified School District (LAUSD) last
month, the Department leveraged a new intra-agency cybersecurity working group to
quickly establish a "Cyberhelp" website highlighting the most impactful cybersecurity
resources from across the Department to support school districts and other
stakeholders to prepare for and respond to cybersecurity incidents. The Department
will soon add one career staff person who will be focused on cybersecurity- related
matters through our programs in the Office of Safe and Supporting Schools, and also
recently "onboarded" a Digital Infrastructure Fellow in the Office of Educational
Technology, to increase its capacity for formal and informal federal, state, and local
coordination.

GAO made three recommendations to the Department:

Recommendation 1 - The Secretary of Education, in consultation with the Cybersecurity and Infrastructure Security Agency (CISA) and other stakeholders involved in updating the Education Facilities Sector-Specific Plan, should establish a collaborative mechanism, such as an applicable government coordinating council, to coordinate cybersecurity efforts between agencies and the K-12 community.

ED Response: The Department concurs in part with the recommendation regarding the need for collaboration with other federal partners regarding K-12 cybersecurity. Additionally, the Department has already begun informal interagency coordination with other federal partners and stakeholders, including the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Communications Commission (FCC) and the Office of the National Cyber Director, and is considering the use of other collaborative mechanisms. We will work with the other federal partners and stakeholders to help determine the appropriate mechanisms for further activities.

Recommendation 2 - The Secretary of Education should develop metrics for obtaining feedback to measure the effectiveness of Education's K-12 cybersecurity-related products and services that are available for school districts.

ED Response: The Department concurs in part with this recommendation and agrees to explore whether and what metrics may be useful for obtaining feedback to measure the effectiveness of the Department's K-12 cybersecurity-related products and services that are available for school districts.

Recommendation 3 - The Secretary of Education, in coordination with federal and nonfederal stakeholders, should determine how best to help school districts overcome the identified challenges and consider the identified opportunities for addressing cyberthreats, as appropriate.

ED Response: The Department concurs with this recommendation and has begun the process of identifying ways to assist school districts in overcoming challenges to the extent those challenges are appropriate to the federal role. As noted above, the Department has formed an intra-agency coordination working group and also participates in informal and formal federal interagency coordination to provide resources to help school districts. Towards that end, the Department has already developed a webpage of curated resources, including resources for school districts, parents and other stakeholders at http://tech.ed.gov/cyberhelp. The Department is committed to regularly updating this page as well as identifying and developing additional resources focused on this critical topic.

Thank you for your consideration of the Department's feedback on the three recommendations made in GAO's draft report.

Respectfully,

Mark Washington
Deputy Assistant Secretary
Office of Elementary and Secondary Education

Appendix V: Comments from the Department of Homeland Security

**Homeland
Security**

October 6, 2022

David B. Hinchman
Acting Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report GAO-23-105480, "CRITICAL
        INFRASTRUCTURE PROTECTION: Additional Federal Coordination is
        Needed to Enhance K-12 Cybersecurity"

Dear Mr. Hinchman:

Thank you for the opportunity to comment on this draft report. The U.S. Department of
Homeland Security (DHS or the Department) appreciates the U.S. Government
Accountability Office's (GAO) work in planning and conducting its review and issuing
this report.

DHS leadership is pleased to note GAO's recognition of the Cybersecurity and
Infrastructure Security Agency's (CISA's) efforts to enhance cybersecurity at K-12
schools, such as: (1) collaborating to support the Department of Education as the lead for
the Education Facilities Subsector; (2) interactions with stakeholders through the Multi-
State Information Sharing and Analysis Center; and (3) developing and sharing a variety
of cyber security products and resources. CISA remains committed to supporting federal
partners and K-12 institutions as they prepare for and combat cybersecurity threats.

For example, CISA, in collaboration with the Federal Bureau of Investigation, produced a
fact sheet, "Cyber Threats to K-12 Remote Learning Education," dated December 2020,
which provides cybersecurity best practices and additional resources.[1] Further, on
May 24, 2021, CISA, in collaboration with the National Cyber Security Alliance,
developed and hosted a webinar on "K-12 Education Leaders' Guide to Ransomware:

---

[1] https://www.cisa.gov/sites/default/files/publications/Cyber_Threats_to_K-
12_Remote_Learning_Fact_Sheet_15_Dec_508.pdf

Prevention, Response and Recovery" to support school efforts to enhance their cybersecurity posture during distance and hybrid learning conditions.[2]

The draft report contained four recommendations, including one for DHS with which the Department concurs. Enclosed find our detailed response to the recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for GAO's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

<div align="right">

Sincerely,

JIM H CRUMPACKER

Digitally signed by JIM H CRUMPACKER
Date: 2022.10.06 15:12:27 -04'00'

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

</div>

Enclosure

---

[2] https://www.youtube.com/watch?v=h0J7qGSOVa4

<div align="right">2</div>

<div align="center">

**Enclosure: Management Response to Recommendations
Contained in GAO-23-105480**

</div>

GAO recommended that the Secretary of the Department Homeland Security ensure that
the Director of CISA:

Recommendation 4: Develop metrics for measuring the effectiveness of its K-12
cybersecurity-related products and services that are available for school districts and
determine the extent that CISA meets the needs of state and local-level school districts to
combat cybersecurity threats.

Response: Concur. CISA agrees that metrics are necessary to measure the
effectiveness of CISA's cybersecurity products intended for, or used by, K-12
school districts. Accordingly, as CISA continues to leverage existing products and
develop additional products and services for K-12 audiences, CISA Cybersecurity
Division (CSD) will also develop measures to determine the extent to which our
efforts are meeting the needs of state and local-level school districts to combat
cybersecurity threats. In coordination with CISA Strategy, Policy, and Plans, the
results of the measures developed by CISA CSD will be reported back to CISA
leadership to ensure accountability, the continuous enhancement of products and
delivered mechanisms, and an optimal allocation of resources. Estimated
Completion Date: October 31, 2023.

3

Agency Comment Letter

Text of Appendix V: Comments from the Department of Homeland Security

October 6, 2022

David B. Hinchman
Acting Director, Information Technology and Cybersecurity
U.S. Government Accountability Office 441 G Street, NW

Washington, DC 20548

Re: Management Response to Draft Report GAO-23-105480, "CRITICAL INFRASTRUCTURE PROTECTION: Additional Federal Coordination is Needed to Enhance K-12 Cybersecurity"

Dear Mr. Hinchman:

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS or the Department) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

DHS leadership is pleased to note GAO's recognition of the Cybersecurity and Infrastructure Security Agency's (CISA's) efforts to enhance cybersecurity at K-12 schools, such as: (1) collaborating to support the Department of Education as the lead for the Education Facilities Subsector; (2) interactions with stakeholders through the Multi- State Information Sharing and Analysis Center; and (3) developing and sharing a variety of cyber security products and resources. CISA remains committed to supporting federal partners and K-12 institutions as they prepare for and combat cybersecurity threats.

For example, CISA, in collaboration with the Federal Bureau of Investigation, produced a fact sheet, "Cyber Threats to K-12 Remote Learning Education," dated December 2020, which provides cybersecurity best practices and additional resources.1 Further, on

May 24, 2021, CISA, in collaboration with the National Cyber Security Alliance, developed and hosted a webinar on "K-12 Education Leaders' Guide to Ransomware:

Prevention, Response and Recovery" to support school efforts to enhance their cybersecurity posture during distance and hybrid learning conditions.2

The draft report contained four recommendations, including one for DHS with which the Department concurs. Enclosed find our detailed response to the recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for GAO's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Enclosure: Management Response to Recommendations Contained in GAO-23-105480

GAO recommended that the Secretary of the Department Homeland Security ensure that the Director of CISA:

Recommendation 4: Develop metrics for measuring the effectiveness of its K-12 cybersecurity-related products and services that are available for school districts and determine the extent that CISA meets the needs of state and local-level school districts to combat cybersecurity threats.

Response: Concur. CISA agrees that metrics are necessary to measure the effectiveness of CISA's cybersecurity products intended for, or used by, K-12 school districts. Accordingly, as CISA continues to leverage existing products and develop additional products and services for K-12 audiences, CISA Cybersecurity Division (CSD) will also develop measures to determine the extent to which our efforts are meeting the needs of state and local-level school districts to combat cybersecurity threats. In coordination with CISA Strategy, Policy, and Plans, the results of the measures developed by CISA CSD will be reported back to CISA leadership to ensure accountability, the continuous enhancement of products and delivered mechanisms, and an optimal allocation of resources. Estimated Completion Date: October 31, 2023.

1 https://www.cisa.gov/sites/default/files/publications/Cyber_Threats_to_K-12_Remote_Learning_Fact_Sheet_15_Dec_508.pdf

2 https://www.youtube.com/watch?v=h0J7qGSOVa4

Appendix VI: GAO Contacts and Staff Acknowledgments

GAO Contacts

David B. Hinchman at (214) 777-5719 or hinchmand@gao.gov

Staff Acknowledgments

In addition to the contact named above, Michael W. Gilmore (Assistant Director), Kavita Daitnarayan (Analyst-In-Charge), Anna Bennett, Ash Harper, Andrew Yarbrough, Chris Businsky, Priscilla Smith, Ahsan Nasar, and Walter Vance made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548