



October 2021

CRITICAL INFRASTRUCTURE PROTECTION

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

Accessible Version



A Century of Non-Partisan Fact-Based Work

GAO Highlights

Highlights of [GAO-22-105024](#), a report to congressional requesters

Why GAO Did This Study

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

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

What GAO Recommends

GAO is making two recommendations for Education to initiate a meeting with CISA to determine how to update its sector-specific plan and determine whether sector-specific guidance is needed.

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

October 2021






CRITICAL INFRASTRUCTURE PROTECTION

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

What GAO Found

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

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

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

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

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

K-12 cyberattack type	Example of a federal resource
Data Breach	The Department of Education issued a data breach scenario training kit.
Ransomware	The Cybersecurity and Infrastructure Security Agency issued a guide, for ransomware prevention and response.
Business Email Compromise	The Federal Bureau of Investigation issued a notice on the use of malicious emails to compromise the business operations of organizations, and potential mitigations.

K-12 cyberattack type	Example of a federal resource
Distributed Denial-of-Service	The Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigations, and the Multi-State Information Sharing and Analysis Center jointly issued an alert, which described the threat that distributed denial-of-services attacks can pose to K-12 schools and potential mitigations.
Video Conferencing Disruptions	The Cybersecurity and Infrastructure Security Agency issued a document detailing the vulnerabilities in video conferencing and potential mitigations.

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

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

Contents

GAO Highlights		2
	Why GAO Did This Study	2
	What GAO Recommends	2
	What GAO Found	2
<hr/>		
Letter		1
	Background	3
	Federal Agencies Have Provided Cybersecurity Support to K-12 Schools but Have Not Kept Plans Up-to-Date or Determined the Need for Sector-Specific Guidance	16
	Conclusions	26
	Recommendations for Executive Action	27
	Agency Comments and Our Evaluation	27
<hr/>		
Appendix I: Objective, Scope, and Methodology		31
Appendix II: Federal Products, Services, and Support		34
Appendix III: Comments from the Department of Education		36
	Text of Appendix III: Comments from the Department of Education	39
<hr/>		
Appendix IV: GAO Contacts and Staff Acknowledgments		42
	GAO Contacts	42
	Staff Acknowledgments	42
<hr/>		
Tables		
	Text of Federal Resources for Cyberattacks on Kindergarten through Grade 12 (K-12) Schools	2
	Table 1: Cyber Threat Actors	6
	Table 2: Examples of Recent Cyberattacks at Kindergarten through Grade 12 Schools	7
	Text of Figure 1: National Institute of Standards and Technology Cybersecurity Framework Functions and Categories	11
	Table 3: Federal Products, Services, and Support That Address National Institute of Standards and Technology Framework Functions for the Education Facilities Subsector	34

Figure

Federal Resources for Cyberattacks on Kindergarten through Grade 12 (K-12) Schools	2
Figure 1: National Institute of Standards and Technology Cybersecurity Framework Functions and Categories	11

Abbreviations

CISA	Cybersecurity and Infrastructure Security Agency
COPPA	Children's Online Privacy Protection Act of 1998
COVID-19	Coronavirus Disease 2019
DHS	Department of Homeland Security
FBI	Federal Bureau of Investigation
FERPA	Family Educational Rights and Privacy Act of 1974
GSA	General Services Administration
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 Secure Schools
PPD-21	Presidential Policy Directive 21
PPD-41	Presidential Policy Directive 41
SRMA	sector risk management agencies
SSP	sector-specific plan

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

October 13, 2021

Congressional Requesters

Many kindergarten through grade 12 (K-12) schools moved from in-person to remote education when the Coronavirus Disease 2019 (COVID-19) pandemic forced the closure of schools across the nation.¹ Remote education has increased K-12 schools' dependence on IT, such as laptops, wireless internet access, and cameras and microphones.

Such reliance on IT increases the vulnerability of K-12 schools to potentially serious cyberattacks. Schools across the nation have increasingly reported various types of cyberattacks. The growing number of cyberattacks on schools highlights the importance of securing K-12 schools information technology.

Ensuring the cybersecurity of the nation has been on our 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 We later identified ensuring national cybersecurity as one of nine high-risk areas that need especially focused executive and congressional attention.⁴

You asked us to review cybersecurity at K-12 schools. The objective of this review—the first of two reviews planned in response to your

¹K-12 includes all public, private, and charter schools from kindergarten through 12th grade. In this report, we collectively refer to all these different types of schools as “K-12 schools.”

²GAO, *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.

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

⁴GAO, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, [GAO-19-157SP](#) (Washington, D.C.: Mar. 6, 2019).

request—is to determine the extent to which federal agencies have assisted schools in protecting themselves from cyber threats. We plan to initiate a second review to assess states' use of federal assistance to combat cyber threats at K-12 schools and what further assistance might be needed.

To address the objective of this review, we examined relevant law and federal guidance, such as the National Defense Authorization Act (NDAA) for Fiscal Year 2021, the *National Infrastructure Protection Plan* (National Plan), and Presidential Policy Directive 21 (PPD-21). These authorities specify the roles and responsibilities of the Department of Homeland Security (DHS), the Department of Education, and the Federal Bureau of Investigation (FBI) to assist K-12 schools in protecting against cyber threats.⁵ DHS's Cybersecurity and Infrastructure Security Agency (CISA) and Education's Office of Safe and Secure Schools (OSSS) are the department-designated agencies responsible for assisting K-12 schools in defending against cyber threats.⁶

We also collected and analyzed documentation of the types of support these agencies offer to K-12 schools, and we interviewed officials from the agencies about the programs, services, and products they offer to assist schools. We compared the activities these agencies undertook to plan for and provide assistance to support schools with the roles and responsibilities of the agencies, as defined in laws and guidance, and identified any gaps in the agencies' efforts to fulfill their roles and

⁵Department 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. PPD-21 establishes requirements for sector-specific agencies and DHS. The fiscal year 21 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.

⁶The Education Facilities Sector-Specific Plan designates the department's Office of Safe and Drug Free Schools as the sector risk management agency (SRMA) for the Education Facilities Subsector. Department of Homeland Security and Department of Education, *Education Facilities Sector-Specific Plan: An Annex to the Government Facilities Sector-Specific Plan* (2010). Department of Education officials stated that this office is now known as the Office of Safe and Supportive Schools (OSSS). In addition, the Cybersecurity and Infrastructure Security Agency Act of 2018 created CISA, within the Department of Homeland Security. Pub. L. No. 115-278, title XXII, 132 Stat. 4168-4186 (Jan. 3, 2018). As such, DHS responsibilities for the protection of critical infrastructure were assigned to CISA.

responsibilities. We discussed our assessment with agency officials from CISA, OSSS, and the FBI to determine the reasons for any apparent gaps in agency efforts.

In addition, we compared planning documents, such as the Education Facilities and Government Facilities Sector-Specific Plans (SSPs) to GAO's key characteristics of a national strategy to further identify gaps in the agencies' efforts to fulfill their roles and responsibilities in supporting the Education subsector.⁷

We further identified significant threats facing the subsector by analyzing K-12 cyber incidents that were identified in a prior GAO report.⁸ We analyzed the Education Facilities SSP to determine the extent to which it addressed these and other types of cyber threats facing the subsector. We discussed our assessment of the subsector plan with OSSS and CISA officials to determine the reasons for apparent gaps in agency planning efforts. Appendix I discusses our objectives, scope, and methodology in greater detail.

We conducted this performance audit from February 2021 to October 2021 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

Our nation's critical infrastructure refers to the 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. DHS has identified 16 critical infrastructure sectors,

⁷GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, [GAO-04-408T](#) (Washington, D.C.: Feb. 3, 2004).

⁸GAO, *Data Security: Recent K-12 Data Breaches Show That Students Are Vulnerable to Harm*, [GAO-20-644](#) (Washington, D.C.: Sept. 15, 2020).

including the Dams Sector; the Nuclear Reactors, Materials, and Waste Sector; and the Government Facilities Sector.⁹

In 2013, DHS established the National Plan, to guide protection efforts in the sectors. The National Plan designated Education Facilities, including K-12 schools, as a subsector of the Government Facilities Sector.¹⁰ In addition to educational facilities, the Government Facilities Sector includes facilities owned or operated by the 56 states and territories, 3,031 counties, 85,973 local governments, 566 federally recognized tribal nations, and the more than 900,000 public and non-public facilities owned or operated by the federal government. Collectively, this sector is one of the largest and most complex sectors within the 2013 National Plan framework.

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.¹¹ According to the K-12 Security Information Exchange (K12 SIX), a non-profit information sharing organization, K-12 is a \$760 billion sector that serves over 50 million students.¹²

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

⁹The other sectors include: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Healthcare and Public Health; Information Technology; Transportation Systems; and Water and Wastewater Systems.

¹⁰Department of Homeland Security, *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: December 2013). The National Plan identified 16 critical infrastructure sectors vital to the United States. In addition, the plan identified the Department of Education as the SRMA and designated Education Facilities as a subsector of the Government Facilities Sector. The Education Facilities SSP describes this designation as including K-12 schools.

¹¹The scope of our review was limited to K-12 schools.

¹²Established in late 2020 as an affiliate of the Global Resilience Federation, K-12 SIX uses data and analytics tools to help schools prevent cyber threats and mitigate cyber incidents that occur by providing alerts, reports, document libraries, and discounted access to security tools.

educational technology vendors¹³, collect and store a range of information about students in these systems and networks. Further, grades, test scores, addresses, telephone numbers, emails, Social Security numbers and medical information are also collected and stored in these systems. With greater connectivity among these systems and networks, threat actors are increasingly motivated to attack these systems for financial gain, to disrupt classes, or for other potentially destructive purposes.¹⁴

Increased Threat of Cyberattacks at K-12 Schools

K-12 schools across the nation face a range of cybersecurity threats. From 2018 to the present, schools in most states have reported cyberattacks on their systems.¹⁵ In 2020, at least 408 cyber incidents at K-12 schools were publically reported—an 18 percent increase over the previous year.¹⁶

Increased usage of IT by K-12 schools to conduct remote learning, in addition to the IT systems commonly used before the COVID-19 pandemic, have increased the potential for a cyberattack as threat actors view schools as opportunistic targets. These threat actors may be motivated by the promise of monetary gain from malware attacks, 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) have noted that threat actors target K-12 remote education to cause disruptions and steal data.¹⁷ Further, the 2019 U.S. Intelligence Community Worldwide Threat Assessment and the 2020 Homeland Threat Assessment state that foreign nations and criminal groups pose

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

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

¹⁵Some cyberattacks on K-12 schools may not be publicly reported.

¹⁶K-12 Cybersecurity Resource Center and the K12 Security Information Exchange, *The State of K-12 Cybersecurity: 2020 Year in Review*, (Mar. 10, 2021). Incidents were assigned to individual school districts regardless of whether an attack affects one school district or many.

¹⁷Cybersecurity 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, 2021, <https://us-cert.cisa.gov/ncas/alerts/aa20-345a>.

the greatest cyberattack threats to critical infrastructure.¹⁸ 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.

Table 1: Cyber Threat Actors

Threat actor	Description
Criminal groups	Criminal groups, including organized crime organizations, seek to use cyberattacks for monetary gain. According to the 2020 Homeland Threat Assessment, cybercriminals increasingly target critical infrastructure to generate profit. That 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 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, they 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. 2021), and relevant federal documents. | GAO-22-105024

These threat actors conduct cyberattacks using various methods, including ransomware, video conferencing disruptions, denial-of-service attacks, and phishing. Table 2 describes publicly reported examples of such attacks.

¹⁸The 2019 Worldwide Threat Assessment of the U.S. Intelligence Community notes the cyber risk of terror organizations, in addition to nations and criminal groups. However, the more recent 2020 Homeland Threat Assessment does not identify terrorists as one of the top cyber threats facing the nation’s critical infrastructure.

Table 2: Examples of Recent Cyberattacks at Kindergarten through Grade 12 Schools

Cyberattack	Description	Example
Ransomware	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.	In March 2021, the Broward County, Florida school district with more than 260,000 students was victim to a ransomware attack carried out by a criminal group. The group encrypted the school district's data and demanded a \$40 million ransom to decrypt the data.
Video Conferencing Disruption	Video Conferencing Disruptions are disruptions of teleconferences and online classrooms, often with pornographic or hate images and threatening language.	In September 2020, an unauthorized individual was unknowingly admitted to an elementary school video meeting. The individual disrupted the meeting for approximately 1 minute by displaying pornographic images to students.
Denial-of-Service	A Denial-of-Service attack is one that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.	In September 2020, the Miami-Dade County, Florida school district was victim to a series of denial-of-service attacks that disrupted learning and teaching on the district's networks and web-based systems.
Phishing	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.	In April 2019, the Scott County, Kentucky school district was victim to a phishing scam, in which the attacker sent a fraudulent email disguising themselves as a vendor. The school district mistakenly paid a \$3.7 million invoice to the attackers.

Source: GAO analysis of relevant Federal and local government documents, and news articles. | GAO-22-105024

We previously reported that K-12 schools and their vendors are increasingly subject to data breaches.¹⁹ These data breaches can include

¹⁹GAO, *Data Security: Recent K-12 Data Breaches Show That Students Are Vulnerable to Harm*, [GAO-20-644](#) (Washington, D.C.: Sept. 15, 2020).

compromises of academic records, students' personally identifiable information, and health or medical information. Breaches of these types of data can pose significant financial harm to students, as well as physical and emotional harm, if personal information is disclosed to other students. Cyberattacks that are carried out on vendors and partners can have a severe effect, as vendors frequently serve many students across multiple schools.

According to data from K12 SIX, K-12 schools publicly reported 62 ransomware incidents in 2019, compared to 11 ransomware incidents reported in 2018.²⁰ In addition, the data notes that 75 percent of all data breaches at K-12 schools in 2020 were carried out on schools' vendors. These attacks further increased during the COVID-19 pandemic.

Further, according to MS-ISAC data, reported ransomware incidents against K-12 schools increased significantly at the beginning of the 2020 school year. Specifically, in August and September 2020, 57 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 previous 2019 school year from January through July of 2020.

Federal Law and Policies Establish Requirements for Critical Infrastructure Protection

Federal law and public-private plans establish roles and responsibilities for the protection of critical infrastructure, including the Education Facilities Subsector. Key law and policies include the National Defense Authorization Act (NDAA) for fiscal year 2021; Executive Order 13636; the National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity; Presidential Policy Directives 21 and 41; Presidential Decision Directive 63; the National Plan; and the Government Facilities Sector-Specific Plan (SSP). These are discussed in more detail below.

²⁰K12 SIX began collecting data on cyber incidents, including ransomware, in 2016 and does not have data prior to that year.

Executive Order 13636

In February 2013, the White House issued *Improving Critical Infrastructure Cybersecurity*, Executive Order 13636.²¹ This order called for a partnership with the owners and operators of critical infrastructure to improve cybersecurity-related information sharing. To do so, the order established mechanisms for promoting engagement between federal and private organizations, including government-coordinating councils that include federal agencies with responsibilities related to critical infrastructure protection and sector coordinating councils that include private-sector entities with roles in protecting critical infrastructure sectors.

Among other things, the Executive Order designated federal sector-specific agencies, now renamed as sector risk management agencies (SRMA) by the fiscal year 2021 NDAA.²² The SRMAs serve as the lead agencies for coordinating federally sponsored activities within their sectors. Further, the order directed 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.

Executive Order 13636 directed NIST to lead the development of a flexible performance-based cybersecurity framework that was to include a set of standards, procedures, and processes.²³ Finally, the order also directed SRMAs, in consultation with DHS and other interested agencies,

²¹The White House, *Improving Critical Infrastructure Cybersecurity*, Executive Order 13636 (Washington, D.C.: Feb. 12, 2013).

²²The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Fiscal Year 2021 NDAA), Pub. L. No. 116-283, section 9002(a)(7), substituted the term “Sector Risk Management Agency” for “Sector-Specific Agency” in the definitions in section 2201(5) of the Homeland Security Act of 2002 (6 U.S.C. § 651(5)). Section 9002 also made conforming amendments and other changes to critical infrastructure sector designation elsewhere in the Homeland Security Act (see 6 U.S.C. § 652a). The NDAA also added a new section 2215, Sector Risk Management Agencies, that includes the responsibilities of those agencies, to the Homeland Security Act (codified at 6 U.S.C. § 665d). See also, 15 U.S.C. § 272(e)(3)(B) for definitions of “critical infrastructure” (42 U.S.C. § 5195c(e)) and “Sector-Specific Agency” (now Sector Risk Management Agency) applicable to NIST’s responsibilities.

²³The Cybersecurity Enhancement Act of 2014 authorized NIST to facilitate and support the development of a voluntary set of standards to reduce cyber risks to critical infrastructure. 15 U.S.C. § 272(c)(15). The *Framework for Improving Critical Infrastructure Cybersecurity* represents that voluntary set of standards.

to coordinate with Sector Coordinating Councils to review the cybersecurity framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments.

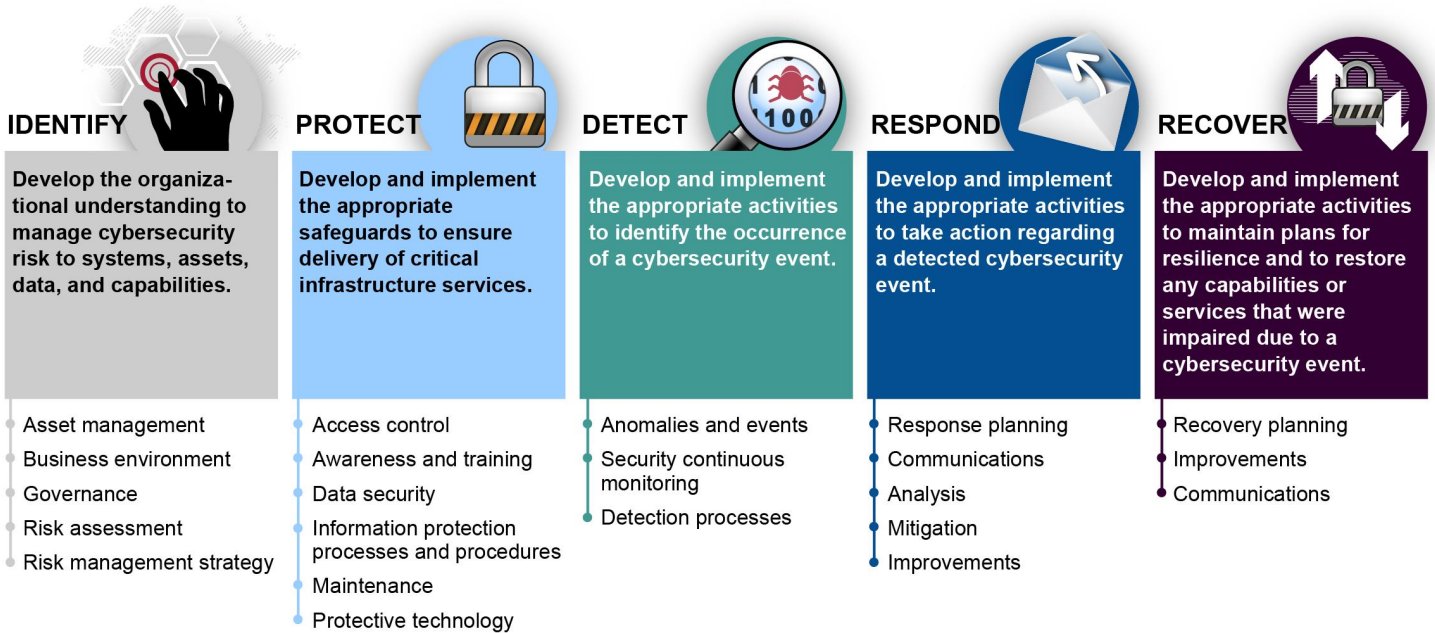
Framework for Improving Critical Infrastructure Cybersecurity

In response to Executive Order 13636, NIST first published, in February 2014, the *Framework for Improving Critical Infrastructure Cybersecurity*, a voluntary, flexible, performance-based framework of cybersecurity standards and procedures.²⁴ The framework, which was updated in April 2018, outlines a risk-based approach to managing cybersecurity that 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. In addition, it specifies that organizations should assess security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome. Figure 1 lists the five functions and 22 categories of the framework core.

²⁴National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Washington, D.C.: April 2018).

Figure 1: National Institute of Standards and Technology Cybersecurity Framework Functions and Categories



Source: GAO description of National Institute of Standards and Technology documents. | GAO-22-105024

Text of Figure 1: National Institute of Standards and Technology Cybersecurity Framework Functions and Categories

- **IDENTIFY:** Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
 - Asset management
 - Business environment
 - Governance
 - Risk assessment
 - Risk management strategy
- **Protect:** Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
 - Access control
 - Awareness and training
 - Data security
 - Information protection processes and procedures

- Maintenance
- Protective technology
- **Detect:** Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
 - Anomalies and events
 - Security continuous monitoring
 - Detection processes
- **Respond:** Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
 - Response planning
 - Communications
 - Analysis
 - Mitigation
 - Improvements
- **Recover:** Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.
 - Recovery planning
 - Improvements
 - Communications

Source: GAO description of National Institute of Standards and Technology documents. | GAO-22-105024

Presidential Directives

In February 2013, the White House issued Presidential Policy Directive 21 (PPD-21), *Critical Infrastructure Security and Resilience*, to further specify critical infrastructure responsibilities.²⁵ Among other things, PPD-21 established roles and responsibilities for DHS, the overall lead federal agency for national policy regarding critical infrastructure security and resilience, and for SRMAs. PPD-21 required DHS, in coordination with the SRMAs to (1) develop a description of functional relationships across the federal government related to critical infrastructure security and

²⁵White House, *Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience*, (Washington, D.C.: Feb. 12, 2013).

resilience; (2) conduct an analysis and recommend options for improving public-private partnership effectiveness; and (3) update the National Plan to include the identification of a risk management framework to strengthen the security and resilience of critical infrastructure.

In addition, Presidential Policy Directive 41 (PPD-41), *United States Cyber Incident Coordination*, sets forth principles governing the federal government's response to any cyber incident, whether involving government or private-sector entities.²⁶ According to the directive, federal agencies are to undertake three concurrent lines of effort when responding to any cyber incident: threat response;²⁷ asset response;²⁸ and intelligence support and related activities.²⁹ In addition, when a federal agency is an affected entity, the directive states it is to undertake a fourth concurrent line of effort to manage the effects of the cyber incident on its operations, customers, and workforce.

Further, in May 1998, the White House issued Presidential Decision Directive 63, *Protecting America's Critical Infrastructures*.³⁰ The directive introduced and promulgated the concept of sector-specific Information Sharing and Analysis Centers (ISACs), which are intended to help critical infrastructure owners and operators protect facilities, personnel, and

²⁶White House, *Presidential Policy Directive/PPD-41: United States Cyber Incident Coordination* (Washington, D.C.: July 26, 2016).

²⁷Threat response activities include conducting appropriate law enforcement and national security investigative activity at the affected entity's site; collecting evidence and gathering intelligence; providing attribution; linking related incidents; identifying additional affected entities; identifying threat pursuit and disruption opportunities; developing and executing courses of action to mitigate the immediate threat; and facilitating information sharing and operational coordination with asset response.

²⁸Asset response activities include furnishing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents; identifying other entities that may be at risk and assessing their risk of the same or similar vulnerabilities; assessing potential risks to the sector or region, including potential cascading effects, and developing courses of action to mitigate these risks; facilitating information sharing and operational coordination with threat response; and providing guidance on how best to utilize federal resources and capabilities in a timely, effective manner to speed recovery.

²⁹Intelligence support and related activities facilitate the building of situational threat awareness and sharing of related intelligence; the integrated analysis of threat trends and events; the identification of knowledge gaps; and the ability to degrade or mitigate adversary threat capabilities.

³⁰White House, *Presidential Decision Directive 63: Protecting America's Critical Infrastructures* (Washington, D.C.: May 22, 1998).

customers from cyber and physical security threats and other hazards. ISACs are non-profit, member-driven organizations formed by critical infrastructure owners and operators to share information between government and industry.

The National Defense Authorization Act for Fiscal Year 2021

The fiscal year 2021 NDAA establishes roles and responsibilities for SRMAs in protecting the 16 critical infrastructure agencies in addition to those outlined in PPD-21.³¹ As established by the NDAA, SRMAs are required to (1) coordinate with DHS and collaborate with critical infrastructure owners and operators, regulatory agencies, and others; (2) support sector risk management, in coordination with CISA; (3) assess sector risk, in coordination with CISA; (4) coordinate the sector, including by serving as a day-to-day federal interface for the prioritization and coordination of sector-specific activities; and (5) support incident management, including supporting CISA, upon request, in asset response activities.

Federal Infrastructure Protection Plans

In response to PPD-21, DHS, with the help of private industry and federal agencies within designated sectors, issued an update to the National Plan in 2013.³² The National Plan, intended 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.

According to the National Plan, the critical infrastructure community should work jointly to set specific national priorities. In turn, the national priorities should be supplemented by various sector activities. In addition, the national priorities are to be supported by objectives and priorities developed at the sector level. The National Plan further states that sector objectives and priorities may be articulated in sector-specific plans, which

³¹The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 9002.

³²Department of Homeland Security, *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: December 2013).

are to serve as targets for collaborative planning between SRMAs and their sector partners.

The current version of the Government Facilities SSP was developed in 2015 by the General Services Administration (GSA) and DHS in response to PPD-21 and the 2013 version of the National Plan.³³ The Government Facilities SSP was developed to help understand evolving risks and threats such as cyber risk to the Government Facilities Sector's assets and functions. The GSA and DHS's Federal Protective Service are to update the Government Facilities SSP based on guidance that CISA provided to the sectors.

Federal Laws Govern Student Data Privacy and Security

Data privacy and data security are connected concepts. Data privacy is the process of appropriately limiting the collection, use, and handling of students' information, and data security is the process of maintaining the confidentiality, integrity, and availability of student data by an organization, such as a school district.³⁴ Federal privacy laws may address both data privacy and data security, or focus on either one. Two relevant federal laws pertain to protecting information about students and children: the Family Educational Rights and Privacy Act of 1974 (FERPA),³⁵ which focuses on data privacy, and the Children's Online Privacy Protection Act of 1998 (COPPA),³⁶ which addresses both privacy and data security.³⁷

- The Department of Education is responsible for enforcing FERPA, which addresses the privacy of personally identifiable information in student education records and applies to all schools that receive funds under an applicable program administered by Education. If

³³General Services Administration and Department of Homeland Security, *Government Facilities Sector-Specific Plan*, 2015.

³⁴The Department of Education stated that it has no legal authority to require general information security standards for K-12 schools and asserted that CISA is the primary federal agency for addressing K-12 cybersecurity. However, as discussed later, CISA is not the primary agency to support cybersecurity protection at K-12 schools but is available to help Education develop needed guidance.

³⁵20 U.S.C. § 1232g.

³⁶15 U.S.C. §§ 6501-6506.

³⁷GAO, *Data Security: Recent K-12 Data Breaches Show That Students Are Vulnerable to Harm*, [GAO-20-644](#) (Washington, D.C.: Sept. 15, 2020).

parents or eligible students believe that their rights under the act have been violated, they may file a formal complaint with Education. In response, Education is required to take appropriate actions to enforce and deal with violations. However, because the department's authority under FERPA is directly related to the privacy of education records, Education's security role is limited to incidents involving potential violations of the act.

- COPPA requires the Federal Trade Commission to issue and enforce regulations concerning children's privacy. The COPPA Rule, which took effect in 2000 and was later amended in 2013, requires operators of covered websites or online services that collect personal information from children under age 13 to provide notice and obtain parental consent, among other things.³⁸ COPPA generally applies to the vendors who provide educational technology, rather than to schools. However, according to the Federal Trade Commission guidance, schools can consent on behalf of parents to the collection of students' personal information if such information is used for a school-authorized educational purpose and for no other commercial purpose.³⁹

In addition to federal laws, state laws set varying requirements for protecting the security of schools and the privacy of personally identifiable information contained in them.⁴⁰

Federal Agencies Have Provided Cybersecurity Support to K-12 Schools but Have Not Kept

³⁸The COPPA Rule is codified at 16 C.F.R. Part 312 and implements the Children's Online Privacy Protection Act of 1998, (15 U.S.C. 6501, et seq.,) which prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet.

³⁹When schools provide consent on behalf of parents under COPPA, there may be FERPA implications as well. However, an exception to FERPA, known as the "school official exception," generally applies. This exception permits the disclosure of personally identifiable information from education records, without parental consent, to vendors with whom schools have outsourced institutional services or functions. The exemption also includes restrictions on vendors' use and disclosure of personally identifiable information.

⁴⁰See for example AR Code § 6-18-109 (Arkansas), CA Educ. Code § 49073.6 (California); MD Educ. Code § 4-131 (Maryland); VA Code § 22.1-287.02 (Virginia).

Plans Up-to-Date or Determined the Need for Sector-Specific Guidance

OSSS, CISA, and the FBI have developed and issued a variety of products and services that are available to the Education subsector to help protect against cyber threats. However, OSSS has not fully met other responsibilities for providing support to the subsector. Specifically, it has not kept its SSP up-to-date and has not considered whether sector-specific guidance is needed to guide schools in implementing the NIST Cybersecurity Framework. Officials from the Department of Education's OSSS said that they have no plans to update their SSP because CISA has not directed them to do so, and OSSS has not determined whether sector-specific guidance is warranted. However, the Department of Education is responsible for updating its subsector plan and determining the need for guidance. Without federal support that is guided by an up-to-date plan and supplemented with appropriate guidance, K-12 schools are less likely to have the federal products, services, and support that can best help protect them from cyberattacks.

Federal Agencies Have Roles and Responsibilities in Supporting the Education Facilities Subsector

Laws and federal guidance establish a framework of roles and responsibilities for OSSS, CISA, and the FBI to support the cybersecurity protection of critical infrastructure, including K-12 schools. The Education Facilities SSP, an annex to the Government Facilities SSP, designates the Department of Education as the SRMA for the Education Facilities Subsector. Within the Department of Education, OSSS has this role.

As the SRMA for the Education subsector, OSSS is required to maintain and update the Education Facilities SSP to, among other things, reflect current risks facing the Education subsector. Guidance requires OSSS to update the SSP every 3 years. OSSS is also required to consult with CISA to make a determination whether sector-specific guidance is needed to guide schools in implementing the NIST Cybersecurity Framework. In addition, leading practices described in GAO's report on combating terrorism suggest that OSSS, in consultation with CISA, should maintain a current assessment of the risks facing the Education

subsector to ensure that federal efforts are appropriately aligned to address current threats.⁴¹

While it is not designated as the primary agency to support cybersecurity protection at K-12 schools, CISA has overall responsibility for coordinating with federal and nonfederal entities to identify, analyze, prioritize, and manage strategic risks to the nation's critical infrastructure.⁴² 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. CISA is also responsible for developing and implementing information sharing programs through which it develops partnerships and shares substantive information with the private sector, and state, local, tribal, and territorial governments. In addition to information sharing initiatives, CISA is tasked with developing resources to help spread awareness about cyber threats, protective measures, and response tactics.

The FBI also has a role in providing support to critical infrastructure entities, including K-12 schools. PPD-41 designates the FBI as the lead federal agency for threat response activities, such as investigating cyberattacks and intrusions across critical infrastructure sectors, including the education subsector. The FBI is responsible for conducting domestic collection, analysis to identify threat actors, and dissemination of cyber threat information. It also is responsible for serving as a focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations within the federal government, as appropriate.

OSSS, CISA, and the FBI Provide Products, Services, and Support to Help K-12 Schools Combat Cyber Threats

OSSS, CISA, and the FBI have provided programs, services, and support to assist K-12 schools in protecting and defending against, and responding to cyber threats.

As the SRMA for the Education subsector, OSSS established a Readiness and Emergency Management for Schools Technical

⁴¹GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, [GAO-04-408T](#) (Washington, D.C.: Feb. 3, 2004).

⁴²*The Cybersecurity and Infrastructure Security Agency Act of 2018* sets responsibilities for CISA. Pub. L. No. 115-278, title XXII, 132 Stat. 4168-4186 (Jan. 3, 2018).

Assistance Center to share guidance, training, tools, and resources for K-12 schools and institutions of higher education. In addition, the department's Office of Planning, Evaluation and Policy Development provides other resources for K-12 schools through its Privacy Technical Assistance Center. Examples of the information provided by these technical assistance centers include:

- Tools developed by schools and higher education emergency managers to improve emergency management, such as sample drills, tabletop exercises, and emergency operations plans, tools and templates.
- Guidance to ensure schools are following cybersecurity best practices for online learning and are adhering to the requirements of the Family Educational Rights and Privacy Act (FERPA) to protect the privacy of students' personally identifiable information. The privacy technical assistance center also provides a data breach response checklist and training kits to assist schools in evaluating and building incident response processes and plans and to help staff be prepared to respond to data breaches.
- Guidance for parents and students on preparing for cyber threats students face online, including exercises and training to help ensure cyber safety during the COVID-19 pandemic. The emergency management technical assistance center provides a list of resources available from government and private entities on topics such as technology safety online, privacy and safety tips, and tools and resources for children.

CISA also provides a variety of products and services to assist K-12 schools and other critical infrastructure entities. Key products and services provided by CISA include:

- Alerts regarding threats to critical infrastructure, including indicators of compromise and recommendations for the mitigation of the threat. For example, CISA provided an alert regarding disruptions to K-12 remote learning classes and data security during the COVID-19 pandemic.⁴³ The alert noted that K-12 organizations may be targeted by attacks utilizing social engineering or technology vulnerabilities and outlined

⁴³This product was co-authored by the FBI, CISA, and MS-ISAC. See appendix II for more detail.

potential mitigations such as best practices for defending against ransomware, distributed-denial-of-service, and malware attacks.

- Incident response assistance upon request, including assessment of the root cause of the incident and mitigation steps to restore systems, recover from an incident, and prevent future incidents.⁴⁴ CISA also provides an incident response report based on its assessment that includes information regarding the impact of the incident on systems and information, and the tools and techniques used by the attacker. The report also generally includes a timeline of the attack and the activities the attacker carried out on compromised systems.
- Voluntary assessments and other services, including assessments of an entity's risk management practices as well as vulnerability scanning, web application scanning, phishing campaign assessment, remote penetration testing, and assessments of an entity's dependencies and risk management practices related to third parties and vendors. For example, remote penetration testing simulates the tactics and techniques that adversaries may use against an entity's systems to identify areas to exploit.
- Training exercises, webinars and workshops, including cybersecurity awareness webinars and discussions of best practices to help prevent incidents and prepare entities to respond if an incident occurs.
- General guidance on topics such as general cybersecurity threats, video conferencing security, and ransomware prevention practices and response.

In addition, CISA provides products and services indirectly to K-12 schools through a cooperative agreement with the MS-ISAC, an independent, non-profit organization that was designated by DHS in 2010 as the cybersecurity ISAC for state, local, tribal, and territorial governments. The MS-ISAC receives funding from CISA, which it uses to provide 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. Products and services offered by the MS-ISAC include:

- The Nationwide Cyber Security Review, offered at no cost to MS-ISAC members. The review is an annual, self-administered, cyber risk assessment intended to help state and local entities assess the effectiveness of and identify gaps in their cybersecurity programs and

⁴⁴CISA only advises organizations on corrective actions, it does not carry out remediation activities.

initiatives. The review is aligned with the NIST Cybersecurity Framework to help entities identify and prioritize actions for reducing cybersecurity risks. According to CISA officials we interviewed, 118 local K-12 organizations participated in the 2019 iteration of this review.⁴⁵

- The Malicious Domain Blocking and Reporting service, offered at no cost to MS-ISAC members, which can help prevent IT systems from connecting to malicious web domains and thus limit infections related to malware, ransomware, and phishing.⁴⁶ According to the MS-ISAC, as of April 2021, 276 of its K-12 members are using this service.
- An around-the-clock cybersecurity operations center that provides information to its members at no cost, including cyber threat intelligence and notices about specific cyber incidents that may affect members.
- An around-the-clock network monitoring service known as “Albert” that analyzes network traffic of participating members to identify threats. According to MS-ISAC officials, fewer than 10 K-12 members use the Albert service.
- Other response services, including emergency conference calls, forensic analysis, log analysis, reverse engineering, and analytical reports on incidents.

The FBI’s primary function is to conduct threat response activities such as investigating cyberattacks across the critical infrastructure sectors. However, the FBI also issues information and alerts about specific cyber threats targeting state, local, tribal, and territorial governments. The FBI coordinates with CISA on many of these products. Alerts have included detailed information of the threat, indicators of compromise, and recommendations for mitigation. In addition, the FBI offers certain types of assistance to K-12 schools who are victims of cyberattacks. Specifically, the FBI can help in attributing the attack to a specific group or individuals and can conduct analysis to determine what other entities may be affected by the incident in order to notify them. The FBI collects and reports information concerning suspected Internet-facilitated criminal activity on its Internet Crime Complaint Center website. The FBI analyzes

⁴⁵The Nationwide Cyber Security Review is also offered to the Elections Infrastructure ISAC at no cost, which DHS funds as part of a cooperative agreement.

⁴⁶The Malicious Domain Blocking and Reporting service is also offered to members of the Elections Infrastructure ISAC at no cost.

this information to identify emerging threats and new trends, and posts public service announcements and alerts about the scams.

The products and services offered by CISA, OSSS, and the FBI can be mapped to the core functions of NIST's Cybersecurity Framework, which is intended to aid organizations in their management of cybersecurity risk and enable risk management decisions. Appendix II shows examples of products, services, and support provided by CISA, OSSS, and FBI that correspond to four of the five core functions of the NIST framework.⁴⁷

Products and services offered by the MS-ISAC, such as the nationwide cyber review and the malicious domain blocking service, are available to all K-12 school districts that are members. There is no cost or other requirement to be a member, and all resources offered by the MS-ISAC through funding from CISA are free to members. However, some services not funded by CISA, such as endpoint security services, penetration testing, managed security services, and vulnerability management services are offered at additional cost.

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. For example, CISA funds two free Albert Network Monitoring services for each state.⁴⁸ However, officials from the MS-ISAC said that less than 10 school districts are utilizing Albert. According to MS-ISAC officials, out of about 15,000 public school districts in the U.S. that are eligible for membership, only 2,372 have chosen to become members as of May 2021.

OSSS Has Not Kept the Education Facilities Subsector Plan Up-to-Date

While the federal government makes a variety of products and services available to the Education subsector to help protect against cyber threats, a key subsector plan is out of date. As previously stated, the fiscal year 2021 NDAA, National Plan, and SSPs establish responsibilities for

⁴⁷The examples of resources provided by CISA, OSSS, and the FBI are not exhaustive. These agencies also provide other products, services, and support that may help address cybersecurity threats at K-12 schools.

⁴⁸Albert is a federally funded Intrusion Detection System that provides network security alerts and helps identify malicious network activity.

SRMAs. The last-published version of the 2010 Education Facilities SSP requires OSSS to update their SSPs every 3 years. In addition, leading practices described in GAO's report on combating terrorism state that such a plan should include, among other things, an assessment of the risks facing the areas the strategy is directed toward and a risk assessment that includes an analysis of the threats to, and vulnerabilities of, critical assets and operations.⁴⁹ These updates can include changes to the entity's programs or activities, oversight structure, organizational structure, personnel, technology and physical environments.

The Education Facilities SSP was developed and issued in 2010 and has never been updated as an independent document. OSSS officials stated that the most recent update to their SSP is included in an annex of the 2015 Government Facilities SSP, which is past the 3-year cycle for SSPs specified in the Education Facilities SSP. Further, the 2010 plan was primarily focused on physical threats to educational facilities, stating that "cyber elements may play a smaller role in the subsector than in other areas."⁵⁰

However, since the issuance of this plan over a decade ago, the cybersecurity risks facing the Education Facilities Subsector have rapidly evolved. As we previously stated, K-12 schools across the country have increasingly been targeted for ransomware and other cyberattacks in recent years. Ransomware incidents in 2020 were more severe than in prior years; with the attacks affecting more students, demanding higher ransoms, and causing class and school cancelations. Officials from both CISA and OSSS acknowledged that the cybersecurity risks facing K-12 schools have changed since the last issuance of their SSP. Officials from CISA said that cyber incidents, like ransomware, are particularly challenging for K-12 schools because of the schools' limited resources, lack of qualified IT and security personnel, and difficulties assessing and evaluating risks.

OSSS officials stated that while the Department of Education is not in a position to respond directly to cyber threats at the school level, they recognize more can be done in terms of planning for and coordinating the implementation of appropriate information security controls throughout the

⁴⁹GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, [GAO-04-408T](#) (Washington, D.C.: February 2004).

⁵⁰Department of Homeland Security and Department of Education, *Education Facilities Sector-Specific Plan: An Annex to the Government Facilities Sector-Specific Plan* (2010).

Education subsector. The officials stated that the department is considering capacity and staffing needs to expand their ability to address cybersecurity threats at K-12 schools. Officials from both CISA and OSSS agreed that the cybersecurity risks facing K-12 schools have changed since the last issuance of their SSP.

According to OSSS officials, the department has not worked on updating its SSP for the Education Facilities Subsector because CISA has not directed them to do so. However, as previously stated, the Education Facilities SSP requires OSSS to update their SSP triennially. Without federal support that is guided by an up-to-date plan reflecting current risks and operational circumstances, K-12 schools are less likely to have the federal products, services, and support that can best help protect them from cyberattacks.

OSSS Has Not Determined the Need for Subsector-Specific Guidance

Executive Order 13636 directed SRMAs, in consultation with DHS and other interested agencies, to coordinate with the Sector Coordinating Councils to review the NIST Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments. The order also directs DHS, in coordination with SRMAs, to establish a voluntary program to support the adoption of the NIST Cybersecurity Framework by owners and operators of critical infrastructure and other entities.⁵¹ The program is intended to enhance critical infrastructure cybersecurity and encourage the adoption of the NIST framework. We previously reported that one of the program's primary missions is to help sector agencies develop guidance for their respective sectors on how to implement the framework.⁵²

CISA has been promoting the implementation of the NIST Framework as a way to strengthen the management of cyber and physical risks to critical infrastructure. CISA has done this, in coordination with other sectors, by issuing sector-specific guidance to critical infrastructure owners and operators so they can better understand and use the

⁵¹The White House, *Improving Critical Infrastructure Cybersecurity*, Executive Order 13636 (Washington, D.C.: Feb. 12, 2013).

⁵²*Critical Infrastructure Protection: Measures Needed to Assess Agencies' Promotion of the Cybersecurity Framework*, [GAO-16-152](#) (Washington, D.C.: December 2015).

framework to (1) assess and improve their respective sector's cyber resiliency; (2) assess their current and target cybersecurity posture; (3) identify gaps in their existing cybersecurity risk management programs; and (4) identify sector-specific tools and resources that map to the NIST Framework. The sectors for which CISA has prepared sector-specific guidance include Commercial Facilities, Chemical, Emergency Services, Critical Manufacturing, Dams, and Nuclear.⁵³

For example, CISA worked with the Commercial Facilities Sector Coordinating Council and Government Coordinating Council to develop the Cybersecurity Framework Implementation Guidance that identified existing cybersecurity tools and resources in the commercial facilities sector and mapped them to the NIST Framework's five core functions: identify, protect, detect, respond, and recover. It identified existing guidance in the sector such as its Stadium Cybersecurity Best Practices Guide and mapped it to the governance and risk assessment categories under the Identify function.⁵⁴ It also mapped the sector's Payment Card Industry Data Security Standards guidance to the anomalies and events, security continuous monitoring, and detection processes subcategories under the Detect function.⁵⁵ Mapping cybersecurity tools to the NIST Framework allows sector operators to identify gaps within their existing cybersecurity programs, and then plan actions to address those gaps.

Despite increased use and reliance by K-12 schools and other entities in the Education Facilities Subsector on IT systems and significant recent cyberattacks, OSSS has not assessed the need for, or consulted with

⁵³The Department of Homeland Security, CISA, *Commercial Facilities Sector Cybersecurity Framework Implementation Guidance* (May 2020); The Department of Homeland Security, CISA, *Chemical Sector Cybersecurity Framework Implementation Guidance* (May 2020); The Department of Homeland Security, CISA, *Emergency Services Sector Cybersecurity Framework Implementation Guidance* (May 2020); The Department of Homeland Security, *Critical Manufacturing Sector Cybersecurity Framework Implementation Guidance* (2015); The Department of Homeland Security, *Dams Sector Cybersecurity Framework Implementation Guidance* (2015); and the Department of Homeland Security, *Nuclear Sector Cybersecurity Framework Implementation Guidance for U.S. Nuclear Power Reactors* (2015).

⁵⁴According to the Commercial Facilities Cybersecurity Framework Implementation Guidance, the Stadium Cybersecurity Best Practices Guide recommends cybersecurity best practices by examining control systems, enterprise systems, and communication systems that stadiums and arenas typically rely on for essential operations.

⁵⁵According to the Commercial Facilities Cybersecurity Framework Implementation Guidance, the Payment Card Industry Data Security Standards guidance establishes worldwide security standards to help organizations that process card payments prevent credit card fraud through increased controls around data and its exposure to compromise.

CISA on, developing sector-specific guidance for implementing the NIST Cybersecurity Framework. CISA officials stated that they are available to help develop sector-specific implementation guidance for the Education sector but that OSSS, as the SRMA for the subsector, must make the determination that such guidance is needed to address the subsector's risks and operating environment. The CISA officials noted that other resources are available through the MS-ISAC that K-12 schools can utilize to measure the maturity of their cyber risk management practices, such as the nationwide review self-assessment process, which is based on the NIST Framework. However, as mentioned previously, relatively few K-12 school districts are members of the MS-ISAC.

OSSS officials said that the department has not made a determination about the need for sector-specific guidance because it relies on CISA to develop guidance related to information security and believes CISA should make such a determination. However, as CISA officials pointed out, OSSS is the SRMA for the subsector and thus is responsible for making the determination. Without a determination of whether sector-specific guidance is needed, OSSS may be less able to assist K-12 schools in protecting against cyber threats, and as a result, schools may be less able to prevent and respond to cyberattacks.

Conclusions

The Department of Education's OSSS, CISA, and FBI have provided a variety of products, services, and guidance to assist K-12 schools in protecting, defending, and responding to cyber threats. However, OSSS has not undertaken a planning effort to assess changes to the risks facing the Education subsector and how federal assistance priorities could be updated to best meet current needs. While the 2010 SSP states that cyber may play a smaller role in the Education subsector, schools have been increasingly targeted for ransomware and other cyberattacks. As a result, OSSS lacks an up-to-date plan based on a current assessment of the cybersecurity risks facing the subsector.

Although the cybersecurity risks facing the subsector have increased significantly, the Department of Education has not consulted with CISA to make a determination on whether sector-specific guidance is needed for K-12 schools to help protect against those risks. As a result, OSSS may be unable to determine whether the products, services, and support currently being offered by the federal government best meet the needs of the Education subsector in protecting K-12 schools from cyber threats.

Given that significant numbers of ransomware and other cyberattacks are disrupting school operations and threatening the privacy and security of student information, it is critical that the federal government's actions be tailored to achieve the greatest possible protection for K-12 schools and students.

Recommendations for Executive Action

We are making the following two recommendations to Education:

The Secretary of Education should initiate a meeting with the Director of CISA to determine how to update its sector-specific plan (SSP) for the Education subsector. The plan should assess and prioritize federal actions to assist K-12 schools in protecting themselves from cyberattacks. (Recommendation 1)

The Secretary of Education should make a determination, in consultation with the Director of CISA and based on current cybersecurity risks, on whether subsector-specific guidance is needed for the Education subsector. (Recommendation 2)

Agency Comments and Our Evaluation

We provided a draft of this report to the Department of Education, CISA, and FBI. In response, we received written comments on the draft from the Department of Education. In addition, all three agencies provided technical comments, which we have incorporated in the report, as appropriate.

In its comments (reprinted in appendix III), Education concurred with our recommendations, but expressed concerns with how they were to be implemented. The department stated that it has no legal authority to require general information security standards for K-12 schools and that CISA is the primary federal agency for addressing K-12 cybersecurity. The department also stated that, in the area of information security, its authority outside of privacy is generally limited to supporting the efforts of CISA.

We do not believe these assertions are inconsistent with our recommendations. However, we revised our recommendation language as well as language in the report to address the department's concerns.

The actions of updating the subsector plan for the Education subsector and determining whether subsector guidance is needed do not require the department to develop information security standards or take other unauthorized actions regarding information security. The department's role is to develop a plan for the Education subsector and to make a determination about the need for more guidance.

Regarding our first recommendation, the department stated that it would work to update its sector plan at the direction of, and with guidance from, CISA with consideration of its limited role and authority to act within the subsector. However, as described in the report, Education's OSSS is the lead for this action. As the SRMA for the Education subsector, OSSS is required to maintain and update the Education Facilities SSP to, among other things, reflect current risks facing the Education subsector. Guidance requires OSSS to update the SSP every 3 years. We continue to believe OSSS should take the lead to update the SSP in coordination with CISA.

In addition, although the department concurred with our recommendation to consult with CISA and to make a determination whether guidance is needed for the subsector, it reiterated that it does not have specific authority to issue information security guidance. We agree that the Department of Education's authority is limited to privacy. However, as discussed in the report, Education is the lead SRMA for the subsector and is thereby responsible for determining the need for additional guidance. Contrary to Education's assertion, DHS's CISA is not the primary agency to support cybersecurity protection at K-12 schools but is available to help develop needed guidance once OSSS, as the SRMA for the subsector, makes the determination that such guidance is needed.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time we will send copies of this report to appropriate congressional committees, the Secretary of Education, the Secretary of Homeland Security, and the Attorney General of the United States. In addition, the report is 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 Nick Marinos at (202) 512-9342 or marinosn@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 IV.

A handwritten signature in black ink that reads "Nick Marinos". The signature is written in a cursive, flowing style.

Nick Marinos
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

Appendix I: Objective, Scope, and Methodology

Our objective was to determine the extent to which federal agencies have assisted kindergarten through grade 12 (K-12) schools in protecting themselves from cyber threats.

To address this objective, we examined relevant laws and federal guidance that specify the roles and responsibilities of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), the Department of Education's Office of Safe and Secure Schools (OSSS), and the Federal Bureau of Investigation (FBI) to assist schools in protecting against cyber threats. These laws and guidance include the relevant parts of the National Defense Authorization Act for Fiscal Year 2021,¹ the National Infrastructure Protection Plan,² the Government Facilities Sector-Specific Plan,³ the Education Facilities Sector-Specific Plan,⁴ Presidential Policy Directive 21,⁵ Presidential Policy Directive 41,⁶ Executive Order 13636,⁷ the National Institute of Standards and

¹*The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021*, Pub. L. No. 116-283, § 9002.

²Department of Homeland Security, *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: December 2013).

³General Services Administration and Department of Homeland Security, *Government Facilities Sector-Specific Plan*, 2015.

⁴Department of Education and Department of Homeland Security, *Education Facilities Sector-Specific Plan*, 2010.

⁵White House, Presidential Policy Directive/PPD-21: *Critical Infrastructure Security and Resilience* (Washington, D.C.: Feb. 12, 2013).

⁶White House, Presidential Policy Directive/PPD-41: *United States Cyber Incident Coordination* (Washington, D.C.: July 26, 2016).

⁷The White House, *Improving Critical Infrastructure Cybersecurity*, Executive Order 13636 (Washington, D.C.: Feb. 12, 2013).

Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity,⁸ and Presidential Decision Directive 63.⁹

We also interviewed officials from these agencies to obtain information and documentation about the programs, services, and products they offer to assist K-12 schools to combat cyber threats, such as training exercises to prepare staff for cyber incident response, alerts and notifications of cyber threats, recommendations for cyber safety, and network monitoring tools. We analyzed this documentation, including FBI Private Industry Notifications and alerts, reports on Multi-State Information Sharing and Analysis Center (MS-ISAC) and CISA's Malicious Domain Blocking and Reporting service, and other documents to identify the purpose of each program, service, or product.

We compared the programs, services, and products these agencies offer to assist schools in combating cyber threats with the roles and responsibilities of the agencies as defined in the previously identified law, and guidance to determine whether there were any gaps in the agencies' efforts to fulfill their roles and responsibilities. In addition, we compared planning documents, such as the Education Facilities and Government Facilities Sector-Specific Plans (SSPs) to GAO's key characteristics of a national strategy to further identify gaps in the agencies' efforts to fulfill their roles and responsibilities in supporting the Education subsector.¹⁰

In addition, we identified significant cybersecurity threats facing the Education subsector by analyzing data from K-12 Security Information Exchange (K-12 SIX), a non-profit information sharing organization, regarding significant K-12 cyber incidents that were analyzed in a prior GAO report.¹¹ For this report, we analyzed the data to identify significant incidents that occurred in each state between 2018 and 2020 and determine the scope of incidents during this time. In addition, we interviewed officials from federal agencies and the MS-ISAC to obtain

⁸National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Washington, D.C.: April 16, 2018).

⁹White House, Presidential Decision Directive 63: *Protecting America's Critical Infrastructures* (Washington, D.C.: May. 22, 1998).

¹⁰GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, [GAO-04-408T](#) (Washington, D.C.: Feb. 3, 2004).

¹¹GAO, *Data Security: Recent K-12 Data Breaches Show That Students Are Vulnerable to Harm*, [GAO-20-644](#) (Washington, D.C.: Sept. 15, 2020).

information about the types of cyber incidents that were reported by K-12 schools from 2018 to present.

We further reviewed and analyzed the Education Facilities SSP to determine the extent to which it reflected an up-to-date plan that addressed those and other cybersecurity threats in the subsector that were identified from the K-12 SIX data. To do so, we compared the department's last planning effort to federal requirements for updating agency SSPs. In addition, we interviewed OSSS and CISA agency officials to identify whether any sector-specific guidance was developed to address subsector risks and operating environment. We discussed our assessment of the subsector plan with OSSS and CISA agency officials to determine the reasons for apparent gaps in agency planning efforts.

We conducted this performance audit from February 2021 to October 2021, 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.

Appendix II: Federal Products, Services, and Support

Table 3 maps the products, services, and support provided by the Cybersecurity and Infrastructure Security Agency (CISA), the Department of Education’s Office of Safe and Supportive Schools and Office of Planning, Evaluation, and Policy Development, and the Federal Bureau of Investigation (FBI) that correspond to four of the five core functions of the National Institute of Standards and Technology (NIST) Cybersecurity Framework. These agencies also provide other products, services, and support that may help address cybersecurity threats at kindergarten through grade 12 schools.

Table 3: Federal Products, Services, and Support That Address National Institute of Standards and Technology Framework Functions for the Education Facilities Subsector

Framework Core Function	Description	Agency	Related Product, Service, or Support
Identify	Identify cybersecurity risks to systems, people, data, and capabilities in the context of the school to prioritize their efforts.	FBI, CISA, and MS-ISAC:	Alert regarding cyber threats to K-12 remote learning ^a
		CISA	Assessments and cybersecurity services (e.g. risk management practices as well as vulnerability scanning, web application scanning, phishing campaign assessment, remote penetration testing, and assessments of an entity’s connections to third parties and vendors)
		MS-ISAC	Nationwide Cybersecurity Review Cybersecurity Operations Center
		Education	Guidance for parents and students regarding cyber threats during online learning (e.g. resources on technology safety online, privacy and safety tips, and tools and resources for children) ^b
		FBI	Internet Crime Complaint Center Annual Cybercrime Report ^c Private Industry Notifications ^d Alerts ^e
Protect	Protect the schools systems, people, data, and capabilities through appropriate safeguards and limits or contain the impact of a potential cybersecurity event.	CISA	Guidance for schools using video conferencing and ransomware prevention practices ^f Training exercises, webinars and workshops, including cybersecurity awareness webinars and discussions of best practices to help prevent incidents

Appendix II: Federal Products, Services, and Support

Framework Core Function	Description	Agency	Related Product, Service, or Support
		CISA and MS-ISAC	Malicious Domain Blocking and Reporting
		Education	Family Educational Rights and Privacy Act and Online Learning Security Best Practices ⁹
			Virtual library of tools for cyber emergency management (e.g. sample drills, tabletop exercises, and emergency operations plans, tools and templates)
			Data breach response training kit
Detect	Detect cyberattacks in an effective and timely manner, using appropriate activities like continuous monitoring capabilities or detection processes.	CISA and MS-ISAC	Albert Network Monitoring Resources
Respond	Respond to a cyberattack using processes to take action regarding a cybersecurity incident and contain the impact of such an incident.	CISA	Response services (e.g. recommendations for remediation and future prevention, and incident response reports)
		MS-ISAC	Response services (e.g. reverse engineering, log analysis, emergency conference calls, forensic analysis, recommendations for mitigation)
		Education	Data breach response check list ^h
		FBI	Incident response, attribution and analysis

Legend: CISA=Cybersecurity and Infrastructure Security Agency;
 FBI=Federal Bureau of Investigation;
 MS-ISAC= Multi-State Information Sharing and Analysis Center;
 K-12=kindergarten through grade 12

Source: GAO analysis of CISA, OSSS, and FBI resources to combat cyber threats at K-12 schools. | GAO-22-105024

^aFederal Bureau of Investigation, the Cybersecurity and Infrastructure Security Agency, and the Multi-State Information Sharing and Analysis Center, *Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data (AA20-345A)*, Dec. 10, 2020, accessed March 15, 2021, <https://us-cert.cisa.gov/ncas/alerts/aa20-345a>.

^bDepartment of Education, *Cyber Safety Quick Links For Protecting Youth: Empowering Students to Become Responsible Digital Citizens and Engage Online Safely*.

^cFederal Bureau of Investigations, Internet Crime Report 2020.

^dFederal Bureau of Investigation, *FBI FLASH: Increase in PYSA Ransomware Targeting Education Institutions (CP-000142-MW)*, (Mar. 16, 2021).

^eFederal Bureau of Investigation, *FBI Private Industry Notification: Business Email Compromise Actors Targeting State, Local, Tribal and Territorial Governments Straining Resources (20210317-001)*, (Mar. 17, 2021).

^fCybersecurity and Infrastructure Security Agency, *Video Conferencing: Guidelines to Keep you and Your Students Safe*, (May. 13, 2020).

^gDepartment of Education, *Student Privacy Policy Office: FERPA and Virtual Learning Related Resources*, (Mar. 2020).

^hDepartment of Education, *PTAC, Data Breach Response Checklist*, (Sept. 2012).

Appendix III: Comments from the Department of Education



UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF ELEMENTARY AND SECONDARY EDUCATION

September 24, 2021

Nick Marinos
Government Accountability Office
Director, Information Technology and Cybersecurity
441 G Street, N.W.
Washington, D.C. 20548

Dear Director Marinos:

Thank you for the opportunity to review and comment on the draft report by the Government Accountability Office (GAO) titled, "Critical Infrastructure Protection: Agencies Should Take Additional Steps to Help Protect K-12 Schools from Cyber Threats (GAO 105024)." I am pleased to respond to the findings and two recommendations to the U.S. Department of Education (Department) under 31 U.S.C. § 720 and to also include technical edits as an enclosure.

Before responding to the findings and recommendations, we want to note that the draft GAO report seems to imply or indicate that the Department has a broader role and authority in K-12 cybersecurity than authorized by law. For example, the Department has no legal authority to require general information security standards for K-12 schools. Our authority in this area is generally limited to Federal privacy, not information security. While privacy and information security overlap in important ways, we do not believe that the Department's privacy authority would allow us to develop general requirements in the area of information security. In our view, this lack of explicit authority has caused some confusion, including in the draft report, and limits the role the Department is able to play in protecting the information and information systems serving the K-12 community. In the area of information security, our authority outside of privacy is generally limited to supporting the efforts of Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA).

The draft GAO report findings and recommendations focus on the Department's contributions to the National Infrastructure Protection Plan (NIPP), which is administered by CISA, and which is more about coordination on facilities than the sorts of threat mitigation and response that the recent K-12 cybersecurity incidents may require. We strongly urge GAO to consider revising the draft GAO report (as well as the recommendations) to more accurately reflect Education's limited K-12 cybersecurity authority, and to also clarify that the primary Federal role for K-12 cybersecurity rests with CISA, which has specific authority in this arena.

We also urge that GAO fully consider our technical comments and those comments in this cover letter as GAO prepares the final report. We hope that our comments provide a fully accurate

Appendix III: Comments from the Department of Education

picture that would help Federal, state, and local governments going forward address the challenges and possible solutions for the changing and potentially hostile cyber environment facing the K-12 community.

Recommendation 1: “The Secretary of Education, in coordination with the Director of CISA, should update its SSP for the Education subsector. The plan should assess and prioritize Federal actions to assist K-12 schools in protecting themselves from cyberattacks.”

Department Response to Recommendation 1:

The Department concurs with this recommendation to the extent it is consistent with the Department’s role in supporting CISA as the primary Federal agency that addresses K-12 cybersecurity. The Department, at the direction of, and with guidance from, the Director of CISA, will work to update its SSP for the Education subsector quadrennially, as directed by the National Infrastructure Protection Plan or NIPP, and with consideration of the limited role and authority the Department has to act within the subsector. See, <https://www.cisa.gov/2015-sector-specific-plans>.

Recommendation 2: “The Secretary of Education should make a determination, in consultation with the Director of CISA and based on current cybersecurity risks, whether subsector-specific guidance is needed for the Education subsector.”

Department Response to Recommendation 2:

The Department concurs with this recommendation to the extent that it would not require the Department to issue guidance beyond the Department’s authority in K-12 cybersecurity, which is further discussed below given that the Department does not have specific authority to establish general K-12 information security standards beyond our privacy authority. However, because we believe that information security threats pose a significant risk to K-12 student privacy, the Department has provided a range of technical assistance activities and guidance on best practices related to important topics such as understanding data security threats, identifying and managing risk, data lifecycle management, breach response activities, and school emergency operation plans. The Department will continue to make these resources available through two technical assistance centers funded by the Department, namely the Privacy and Technical Assistance Center (at <https://studentprivacy.ed.gov/>) and the Readiness and Emergency Management Technical Assistance Center (at <https://rems.ed.gov/>).

**Appendix III: Comments from the Department
of Education**

Please let us know if you have any further questions or need any additional information.

Sincerely,

**Ian
Rosenblum**

Digitally signed by Ian
Rosenblum
Date: 2021.09.24
09:33:34 -0400

Ian Rosenblum
Deputy Assistant Secretary for Policy and Programs
Delegated the Authority to Perform the Functions
and Duties of the Assistant Secretary
Office of Elementary and Secondary Education

Enclosure

Text of Appendix III: Comments from the Department of Education

September 24, 2021

Nick Marinos

Government Accountability Office

Director, Information Technology and Cybersecurity 441 G Street, N.W.

Washington, D.C. 20548

Dear Director Marinos:

Thank you for the opportunity to review and comment on the draft report by the Government Accountability Office (GAO) titled, “Critical Infrastructure Protection: Agencies Should Take Additional Steps to Help Protect K-12 Schools from Cyber Threats (GAO 105024).” I am pleased to respond to the findings and two recommendations to the U.S. Department of Education (Department) under 31 U.S.C. § 720 and to also include technical edits as an enclosure.

Before responding to the findings and recommendations, we want to note that the draft GAO report seems to imply or indicate that the Department has a broader role and authority in K-12 cybersecurity than authorized by law. For example, the Department has no legal authority to require general information security standards for K-12 schools. Our authority in this area is generally limited to Federal privacy, not information security. While privacy and information security overlap in important ways, we do not believe that the Department’s privacy authority would allow us to develop general requirements in the area of information security. In our view, this lack of explicit authority has caused some confusion, including in the draft report, and limits the role the Department is able to play in protecting the information and information systems serving the K-12 community. In the area of information security, our authority outside of privacy is generally limited to supporting the efforts of Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA).

The draft GAO report findings and recommendations focus on the Department’s contributions to the National Infrastructure Protection Plan (NIPP), which is administered by CISA, and which is more about coordination on facilities than the sorts of threat mitigation and response that the recent K-12 cybersecurity incidents

may require. We strongly urge GAO to consider revising the draft GAO report (as well as the recommendations) to more accurately reflect Education's limited K-12 cybersecurity authority, and to also clarify that the primary Federal role for K-12 cybersecurity rests with CISA, which has specific authority in this arena.

We also urge that GAO fully consider our technical comments and those comments in this cover letter as GAO prepares the final report. We hope that our comments provide a fully accurate picture that would help Federal, state, and local governments going forward address the challenges and possible solutions for the changing and potentially hostile cyber environment facing the K-12 community.

Recommendation 1: “The Secretary of Education, in coordination with the Director of CISA, should update its SSP for the Education subsector. The plan should assess and prioritize Federal actions to assist K-12 schools in protecting themselves from cyberattacks.”

Department Response to Recommendation 1:

The Department concurs with this recommendation to the extent it is consistent with the Department's role in supporting CISA as the primary Federal agency that addresses K-12 cybersecurity. The Department, at the direction of, and with guidance from, the Director of CISA, will work to update its SSP for the Education subsector quadrennially, as directed by the National Infrastructure Protection Plan or NIPP, and with consideration of the limited role and authority the Department has to act within the subsector. See, <https://www.cisa.gov/2015-sector-specific-plans>.

Recommendation 2: “The Secretary of Education should make a determination, in consultation with the Director of CISA and based on current cybersecurity risks, whether subsector-specific guidance is needed for the Education subsector.”

Department Response to Recommendation 2:

The Department concurs with this recommendation to the extent that it would not require the Department to issue guidance beyond the Department's authority in K-12 cybersecurity, which is further discussed below given that the Department does not have specific authority to establish general K-12 information security standards beyond our privacy authority. However, because we believe that information security threats pose a significant risk to K-12 student privacy, the Department has provided a range of technical assistance activities and guidance on best practices related to important topics such as understanding data security threats, identifying and

managing risk, data lifecycle management, breach response activities, and school emergency operation plans. The Department will continue to make these resources available through two technical assistance centers funded by the Department, namely the Privacy and Technical Assistance Center (at <https://studentprivacy.ed.gov/>) and the Readiness and Emergency Management Technical Assistance Center (at <https://rems.ed.gov/>).

Please let us know if you have any further questions or need any additional information.

Sincerely,

Ian Rosenblum

Deputy Assistant Secretary for Policy and Programs Delegated the Authority to Perform the Functions and Duties of the Assistant Secretary

Office of Elementary and Secondary Education

Enclosure

Appendix IV: GAO Contacts and Staff Acknowledgments

GAO Contacts

Nick Marinos, (202) 512-9342 or marinosn@gao.gov

Staff Acknowledgments

In addition to the contact named above, John de Ferrari (Assistant Director), Kavita Daitnarayan (Analyst-In-Charge), Anna Bennett, Chris Businsky, Donna Epler, Jennifer Gregory, Ahsan Nasar, Walter Vance, and Drew Yarbrough 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



Please Print on Recycled Paper.