United States Government Accountability Office

Report to Congressional Requesters

November 2023

FEDERAL GRANTS

Numerous Programs Provide Cybersecurity Support to State, Local, Tribal, and Territorial Governments

Accessible Version

GAO-24-106223

GAO Highlights

Highlights of GAO-24-106223, a report to congressional requesters

November 2023

FEDERAL GRANTS

Numerous Programs Provide Cybersecurity Support to State, Local, Tribal, and Territorial Governments

Why GAO Did This Study

SLTT governments provide essential services that are increasingly reliant on the internet, making them vulnerable to various cybersecurity-related risks. The Department of Homeland Security and other federal agencies administer grant programs for these types of governments.

GAO was asked to identify federal grant programs that provide funding to improve cybersecurity for SLTT governments. The objectives for this report are to describe the (1) federal grant programs supporting SLTT governments' cybersecurity, and how much has been awarded for cybersecurity; and (2) actions taken by relevant federal agencies to monitor cybersecurity-related grants, and what challenges, if any, SLTT governments faced with the application process for cybersecurity-related grant programs.

GAO collected and analyzed federal grant data to determine what federal agencies and programs may support SLTT governments' cybersecurity from fiscal years 2019 through 2022. Using these data, GAO identified federal agencies that administer relevant grant programs and interviewed agency officials about these programs. GAO also reviewed federal requirements and policies regarding agencies' responsibilities for monitoring cybersecurity-related grants. Finally, GAO interviewed officials from national associations that represent SLTT governments, Tribal Nations, and agencies to obtain their perspectives on challenges SLTTs faced when applying for federal cybersecurity-related grants.

View GAO-24-106223. For more information, contact David B. Hinchman at (214) 777-5719 or hinchmand@gao.gov, or Tina Won Sherman at (202) 512-8461 or shermant@gao.gov.

What GAO Found

GAO identified 27 federal grant programs managed by eight federal agencies that could be used to fund state, local, tribal, and territorial (SLTT) governments' cybersecurity. None of these grant programs were intended to primarily support cybersecurity activities and these agencies are not required to track amounts specifically used for cybersecurity activities. However, four federal agencies tracked cybersecurity-related expenditures for 10 of the 27 programs. For fiscal years 2019 through 2022, the agencies reported awarding about $827 million (see table) to support cybersecurity-related activities, such as purchasing new software and network equipment. The cybersecurity-related amounts awarded by the remaining 17 grant programs are unknown.

Cybersecurity-Related Grant Award Amounts Tracked by Four Agencies, Fiscal Years 2019 through 2022

Agency	Total cyber amount	Number of grant programs
Federal Emergency Management Agency	$669,858,956	5
Election Assistance Commission	$155,717,827	2
Department of the Interior	$844,106	1
Institute of Museum and Library Services	$708,926	2
Total	**$827,129,815.00**	**10**

Source: GAO analysis of agency grant data. | GAO-24-106223

Agencies have established policies and processes to monitor grant programs. Agency officials stated that they conduct periodic reviews of progress reports and financial reports submitted by grant recipients to ensure the appropriate usage of funds.

Officials from national associations, SLTT government representatives, and agency officials did not identify challenges with applying for the identified grant programs. However, they identified challenges with the federal grant process in general. For example, officials from two national associations, one Tribal Nation, and three federal agencies said that the federal grant application process can be cumbersome for applicants, especially when the applicants are small SLTT governments with a relative lack of expertise in grant writing. Another Tribal Nation said it can be difficult to retain staff who have grant writing expertise.

GAO has previously reported on a wide range of grant-related issues, including long-standing challenges with federal grants management. For example, GAO identified human capital capacity—the extent to which an organization has sufficient staff, knowledge, and technical skills to effectively meet its goals and objectives—as a key factor in successful grants management.

Contents

Tables

Figure

Abbreviations

CFR	Code of Federal Regulations
DHS	Department of Homeland Security
DOI	Department of the Interior
DOJ	Department of Justice
DOL	Department of Labor
DOT	Department of Transportation
EAC	U.S. Election Assistance Commission
EPA	Environmental Protection Agency
FEMA	Federal Emergency Management Agency
IMLS	Institute of Museum and Library Services
SLTT	state, local, tribal, and territorial

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

November 16, 2023

The Honorable Andrew R. Garbarino
Chairman
Subcommittee on Cybersecurity and Infrastructure Protection
Committee on Homeland Security
House of Representatives

The Honorable Anthony P. D'Esposito
Chairman
Subcommittee on Emergency Management and Technology
Committee on Homeland Security
House of Representatives

The Honorable Kat Cammack
House of Representatives

State, local, tribal, and territorial (SLTT) governments provide essential services, including public utilities, healthcare, and public safety. These services are increasingly reliant on the internet, making them vulnerable to various cyber-related risks. The Department of Homeland Security (DHS) and other federal agencies administer a variety of grant programs that provide funding to these types of governments.

To better understand what additional cybersecurity funding resources were available, you requested that we identify federal grant programs that provide funding to improve cybersecurity for SLTT governments. Our specific objectives were to describe (1) federal grant programs that support SLTT governments' cybersecurity and identify the associated amounts awarded for cybersecurity and (2) actions taken by relevant federal agencies to monitor cybersecurity-related grants and identify challenges, if any, SLTT governments faced with the application process for cybersecurity-related grants.

To address our first objective, we analyzed public grant data available on USAspending.gov to identify federal agencies that are responsible for administering federal grant programs that may specifically support or

could support cybersecurity for SLTT governments.[1] Specifically, we conducted a search on USAspending.gov of federal grant programs that included the keyword "cyber" in the grant description, from fiscal years 2019 through 2022. The search resulted in 124 grant programs across 26 federal agencies. We then reviewed each of the descriptions of these 124 programs and identified those programs intending to support cybersecurity enhancements to SLTT governments' information systems. In doing so, we eliminated grant programs for activities such as research and development, scholarships, international concerns, and general workforce development.

Our search and review process resulted in 27 grant programs that support cybersecurity enhancements to SLTT governments' information systems. These 27 programs are managed by eight agencies: the Departments of Interior (DOI), Justice (DOJ), Labor (DOL), and Transportation (DOT); the Election Assistance Commission (EAC); the Environmental Protection Agency (EPA); DHS's Federal Emergency Management Agency (FEMA); and the Institute of Museum and Library Services (IMLS).

For each of the 27 programs, we gathered and analyzed publicly available grant data on USAspending.gov. We then sent a request for information to the federal agency responsible for overseeing each program. This request sought detailed data about each grant program, including a grant program description, the total amount of funding awarded, the total cybersecurity amount awarded, and a description of the cybersecurity activities that were funded. We also requested information on any other relevant grant programs focused on providing cybersecurity support to SLTT governments. We then interviewed officials from these agencies to further understand each of the 27 grant programs that specifically support cybersecurity for SLTT governments.

We independently reviewed the grant data obtained from the agencies and identified the extent to which funds were used for cybersecurity-related activities, and confirmed which grants were within scope. We also interviewed agency officials about the accuracy and completeness of the

[1]For purposes of this audit, we are defining "cybersecurity" as enhancements to assist with the prevention, protection, and restoration of information and information systems, and to ensure their availability, integrity, authentication, confidentiality, and nonrepudiation. To narrow our scope and agency selection, we eliminated those grants from our scope that are determined to have a focus on research and development, scholarships, international concerns, or general workforce development.

data, their data collection methods, and the system that they used to generate the detailed grant data. We determined the grant data were sufficiently reliable for the purposes of describing the grant programs and how funds were used for cybersecurity, and the amount awarded.

To address our second objective, we focused on the same eight agencies. We identified and reviewed federal requirements, agency policies, and grant program documentation regarding federal agencies' roles and responsibilities for monitoring SLTT cybersecurity-related grants and grant programs. For example, we identified and reviewed relevant sections of the federal regulation that established federal agencies' overarching responsibilities for administering and monitoring federal grants.[2]

We also interviewed agency officials to collect information regarding policies and procedures, and actions they have taken to monitor cybersecurity-related grants and coordinate with other federal agencies and nonfederal entities on those grants. We asked officials representing the federal agencies to identify specific agency grant monitoring policies—for example, FEMA's *Preparedness Grant Manual*—and we reviewed those policies to determine whether they included any roles and responsibilities relevant to cybersecurity-related grant programs. We also reviewed agency documents—such as Notices of Funding Opportunity—that prescribe specific requirements for individual grant programs to determine if there were any additional monitoring or coordination requirements related to cybersecurity-related grant programs.[3]

In addition, we interviewed officials that represent SLTT governments to obtain their perspectives on challenges faced by SLTTs when applying for federal cybersecurity-related grants. Specifically, we interviewed officials from three national organizations that represent state, local, and territorial governments—the National Association of Counties, the National Association of State Chief Information Officers, and the National Governors Association. We further interviewed officials from the Multi-

[2]Specifically, we identified and reviewed sections of the Code of Federal Regulations (CFR) Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards related to grant monitoring. For example, see 2 CFR § 200.300 (Statutory and national policy requirements) and 2 CFR § 200.329 (Monitoring and reporting program performance).

[3]Because FEMA's grant programs represent the vast majority of federal grant spending in our scope, we only reviewed the Notices of Funding Opportunity for the relevant FEMA grant programs, such as the Homeland Security Grant Program.

State Information Sharing and Analysis Center about their views on challenges with cybersecurity-related grants.[4] We based our selection of these entities on their existing relationships with SLTT governments and their willingness to participate in our review. Based on referrals from FEMA's Tribal Affairs team, we contacted and interviewed officials representing two Tribal Nations—the Choctaw Nation and Citizen Potawatomi Nation. We requested information from these officials regarding federal efforts to address any challenges SLTT governments identified with the application process for these grant programs. We further asked agency officials to identify any challenges that SLTT governments faced when applying for federal cybersecurity-related grants.

We conducted this performance audit from September 2022 to November 2023 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

Information technology is an important element of SLTT governments' ability to provide for many essential services necessary for a secure society, including government operations, energy and water utilities, education systems, public health, and emergency response. A failure or disruption to SLTT critical infrastructure could result in significant harm, a major public health issue, long-term economic loss, and impacts to other critical infrastructure.

The government facilities critical infrastructure sector includes 56 states and territories, 3,031 counties, 85,973 local governments, and 574

[4]The Multi-State Information Sharing and Analysis Center is an independent, nonprofit organization that DHS designated in 2010 as the cybersecurity Information Sharing and Analysis Center for SLTT governments. It provides services and information sharing to enhance SLTT governments' ability to prevent, protect against, respond to, and recover from cyberattacks and compromises.

federally recognized Tribal Nations.[5] These SLTT governments face a number of threats such as cyber threats, physical threats, and natural disasters.

SLTT governments face a range of cybersecurity dangers from various threat actors using a variety of different methods such as ransomware,[6] denial-of-service,[7] and phishing.[8] The threat actors may be motivated by the promise of monetary gain, by the desire to steal data, or simply to cause disruption. Table 1 summarizes the various types of threat actors.

Table 1: Cybersecurity Threat Actors

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

Sources: Summary of GAO-21-81 and other relevant federal documents. | GAO-24-106223

[5]Department of Homeland Security, *Government Facilities Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan 2013* (2015). This sector-specific plan provides a strategy for federal facility resilience, establishes priorities for enhancing security and resilience for federal facilities, and defines overarching strategic goals, objectives, and actions for the Government Facilities sector.

[6]Ransomware is a form of malicious software designed to encrypt files on a device and render data and systems unusable. Malicious actors then demand ransom payments in exchange for restoring access to the locked data and systems.

[7]A denial-of-service attack is one that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.

[8]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.

SLTT government organizations, including schools, have been particularly targeted by cybersecurity-related incidents such as ransomware, which can have devastating impacts on vital government operations and services. According to the Multi-State Information Sharing and Analysis Center, SLTTs experienced approximately 2,800 ransomware incidents from January 2017 through March 2021. Table 2 summarizes publicly reported examples of such incidents.

Table 2: Examples of State, Local, Tribal, and Territorial (SLTT) Government Cybersecurity-Related Incidents

SLTT entity	Year	Impact description
Des Moines Public Schools (Iowa)	January 2023	The district preemptively shut down its network services in response to unusual activity on the network. The district canceled classes for 2 days while IT staff conducted an investigation to remove any threats to the network.
Los Angeles Unified School District (California)	September 2022	It was reported that the school district—which is the second largest in the country—was victim to a cyberattack by a known ransomware group, resulting in stolen data. After the school district refused to pay a ransom, the ransomware group reported that it had leaked over 500 gigabytes of district employees' sensitive information. In February 2023, it was reported that approximately 2,000 student mental health assessment records had been posted on the dark web.
Chicago Public Schools	December 2021	The district was a victim of a ransomware attack in which more than 500,000 students' and staff members' personal information was disclosed. The data included students' names, schools, dates of birth, genders, school identification numbers, state identification numbers, and course information from previous school years.
Three affiliated tribes – the Mandan, Hidatsa, and Arikara Nation	April 2021	The Tribal Nation was victim to a ransomware attack that ceased access to files, email, and critical information on its server.
Miami-Dade County Public Schools	September 2020	The district was a victim of a series of denial-of-service attacks that disrupted learning and teaching on its networks and web-based systems.
Baltimore City, Maryland	May 2019	The Mayor of Baltimore reported that the city was the victim of a ransomware attack. As a result, city employees were not able to access their emails and the attack delayed real estate sales and water billing for months.

Sources: Published news articles, GAO-22-104767, and GAO-23-105480. I GAO-24-106223

Federal Grants Can Be Used to Bolster Cybersecurity of State, Local, Tribal, and Territorial Governments

The increasing cyber threats and attacks to SLLT entities highlight the importance and need for SLTT governments to strengthen their cybersecurity defenses. Through federal grant programs that may be intended to either directly support cybersecurity activities or are eligible to help support cybersecurity enhancements, among other purposes, the federal government can provide funding assistance to bolster SLTT

governments' cybersecurity resiliency and effectiveness.[9] Awards from these grant programs are in the form of discretionary grants or formula grants:

- **Discretionary grants.** A grant (or cooperative agreement) for which the awarding federal agency generally may select the recipient from among all eligible recipients; decide to make or not make an award based on the programmatic, technical, or scientific content of an application; and decide the amount of funding to be awarded.
- **Formula grants.** A grant in which allocations of federal funding are provided to states, Tribes, territories, or local units of governments as determined by distribution formulas in the authorizing legislation and regulations. To receive a formula grant, the recipient must meet all the eligibility criteria for the program, which are pre-determined and not open to discretionary funding decisions.

Federal Grant Lifecycle

Federal grant programs are generally created by statute and funded through annual appropriations. As such, Congress has a central role in determining the scope and nature of federal financial assistance programs. In addition, the Office of Management and Budget establishes general guidance, which governs administration of all such federal financial assistance, and agencies have flexibility in how to administer assistance that is discretionary in nature.[10]

Generally, federal award-making agencies follow the same grant process when awarding federal grants. According to Grants.gov, the grant process follows a lifecycle that includes creating the funding opportunity, applying, making award decisions, and successfully implementing the award.[11] The specific actions along the lifecycle are grouped into three main phases:

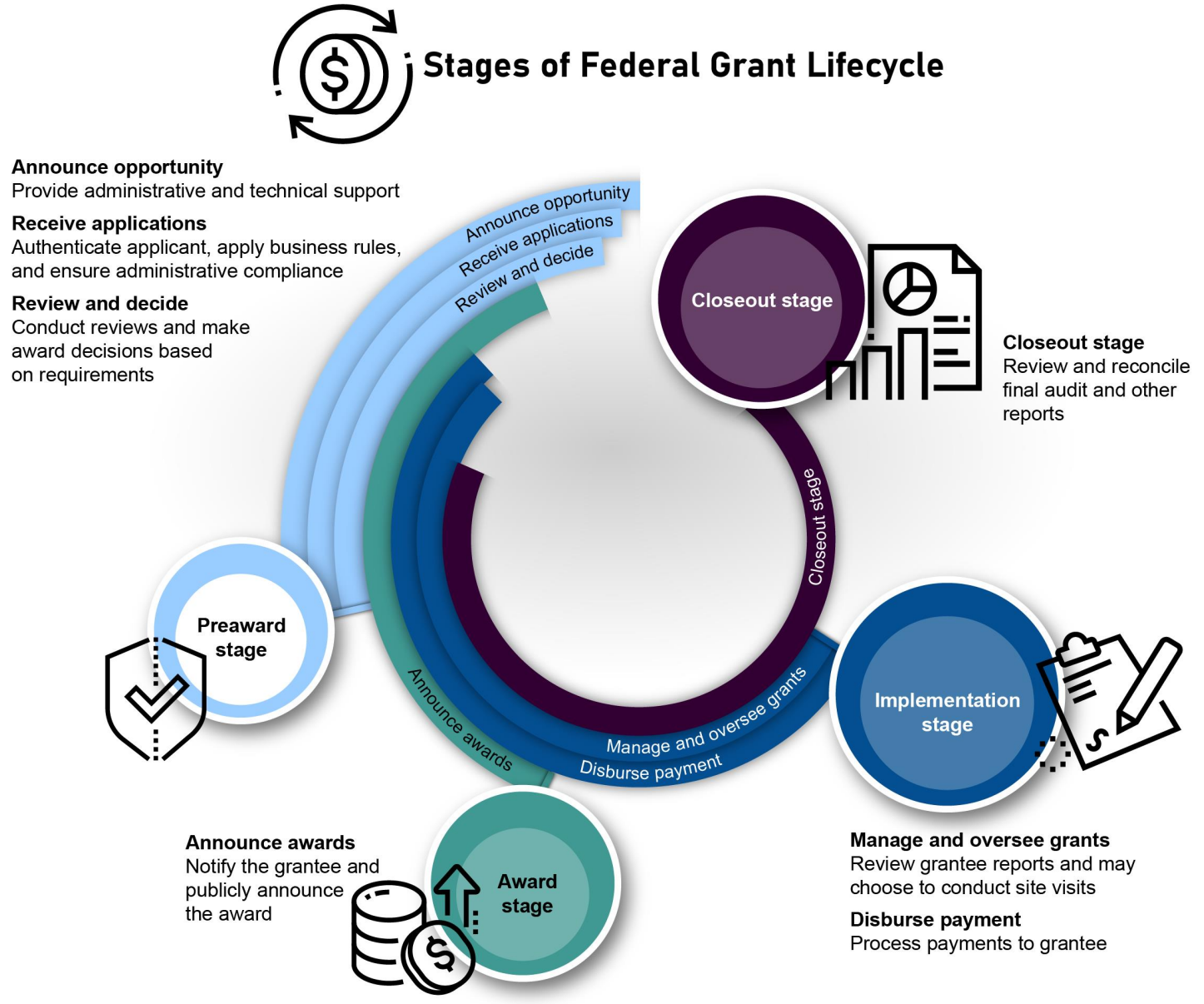
[9]In terms of grants that can be used for cybersecurity, for purposes of this review we are defining "cybersecurity" as enhancements to assist with the prevention, protection, and restoration of information and information systems, and to ensure their availability, integrity, authentication, confidentiality, and nonrepudiation.

[10]While federal agencies do have some discretion in making grant awards, they are subject to federal guidelines found in the grants management common rule. See Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards codified at 2 C.F.R. Part 200.

[11]Established in 2002 as part of the President's Management Agenda and managed by the Department of Health and Human Services, Grants.gov is a website that provides a centralized location for grant seekers to find and apply for federal funding opportunities.

pre-award, award, and post award. The grant lifecycle is shown in figure 1.

Figure 1: Federal Grant Lifecycle



Sources: GAO; palau83/stock.adobe.com (icons). | GAO-24-106223

Accessible text for Figure 1: Federal Grant Lifecycle

Stages of Federal Grant Lifecycle

- Announce opportunity: Provide administrative and technical support
- Receive applications: Authenticate applicant, apply business rules, and ensure administrative compliance
- Review and decide: Conduct reviews and make award decisions based on requirements

- Preaward Stage: Announce awards and notify the grantee and publicly announce the award
- Award Stage
- Implementation stage
  - Manage and oversee grants. Review grantee reports and may choose to conduct site visits
  - Disburse payments. Process payments to grantee.
- Closeout stage. Review and reconcile final audit and other reports

Source GAO. | GAO-24-106233

GAO Has Previously Reported on Federal Grants Management Challenges

We have reported on numerous aspects of federal grants management in past reports and testimony spanning several decades. In a May 2023 testimony, we provided a summary of common themes covered in these prior reports and testimony related to long-standing challenges with grants management, such as issues with capacity and oversight.[12] More specifically:

- **Human capital capacity** is the extent to which an organization has sufficient staff, knowledge, and technical skills to effectively meet its goals and objectives. We reported in May 2023 that officials from three associations representing state and local governments told us that because of the extensive compliance and reporting requirements,

[12]For more information, see GAO, *Grants Management: Observations on Challenges with Access, Use, and Oversight*, GAO-23-106797 (Washington, D.C.: May 2, 2023).

smaller localities that do not regularly receive federal funding assistance may face capacity challenges when managing their allocations because they have fewer staff and less knowledge and awareness of federal processes than larger localities. One way that federal agencies can help organizations mitigate capacity limitations is through technical assistance and by making available federal or other revenue dedicated to covering the cost of grant administration and oversight.

- **Effective oversight** is important to providing reasonable assurance to federal managers and taxpayers that grants are awarded properly, recipients are eligible, and that grant recipients use federal grant funds as intended and in accordance with applicable laws and regulations. In our May 2023 testimony, we stated that we and agency inspectors general identified weaknesses in agencies' internal controls for managing and overseeing grants. Specifically, we found that when such controls are weak, federal grant-making agencies face challenges in achieving grant program goals and assuring the proper and effective use of federal funds to help avoid improper payments. One way that federal agencies oversee nonfederal grantees is through an audit of their expenditures of federal awards and financial statements, which is an important component of a single audit.

Federal Grant Programs Awarded at Least $827 Million to Enhance SLTT Governments' Cybersecurity

We identified 27 federal grant programs across eight federal agencies that could have been used to fund SLTT governments' cybersecurity enhancements. None of the grant programs were intended to support only cybersecurity activities. See table 3 for the agencies and number of programs identified for each. The 27 grant programs are further described in tables 4 to 11.

Table 3: Number of Grant Programs by Agency That Could Fund State, Local, Tribal, and Territorial Cybersecurity Enhancements, Fiscal Years 2019 through 2022

Agency	Number of grant programs
Department of Interior	1
Department of Justice	4
Department of Labor	2
Department of Transportation	9

Agency	Number of grant programs
Election Assistance Commission	2
Environmental Protection Agency	2
Federal Emergency Management Agency	5
Institute of Museum and Library Services	2
Total grant programs	**27**

Source: GAO analysis of agency data. | GAO-24-106223

In addition, during fiscal years 2019 through 2022, the federal government reported awarding at least $827,129,815 across 10 grant programs to SLTT governments to support their cybersecurity-related activities.

Four Agencies Administered 10 Grant Programs That Awarded $827 Million Eligible for Cybersecurity

Four of eight agencies—DOI, EAC, FEMA, and IMLS—tracked cybersecurity-related award amounts across 10 of the 27 federal grant programs identified as being eligible to fund SLTT governments' cybersecurity enhancements.

DOI. DOI administers one grant program that was used to fund SLTT governments' cybersecurity-related activities. During fiscal years 2019 through 2022, DOI reported that it awarded $844,106 to two U.S. territories for cybersecurity-related activities. See table 4 for a description of DOI's grant program and total awarded amounts for cybersecurity-related activities.

Table 4: Department of the Interior Grant Program Awarded Amounts Used for Cybersecurity, Fiscal Years 2019 through 2022

Grant program	Description	Total cybersecurity amount identified
Technical Assistance Program	Provides grant funding for short-term projects intended to meet the immediate needs of the insular areas.	$844,106

Source: GAO analysis of Department of the Interior grant data and related documentation. I GAO-24-106223

Two U.S. territories used funds awarded from the Technical Assistance Program for various cybersecurity-related activities. For example, one U.S. territory purchased software to automate reporting and detect anomalies. Additionally, the other U.S. territory upgraded their systems configuration of switches and routers to align with current IT standards. It also used funds to implement technical controls, establish cybersecurity-

related policies and procedures, and train system technicians and personnel.

EAC. The commission administers two grant programs that were used to fund SLTT governments' cybersecurity-related activities. EAC reported that it awarded $155,717,827 to 44 states and three U.S. territories from fiscal years 2019 through 2022. See table 5 for a list of EAC's grant programs and the cybersecurity amounts.

Table 5: Election Assistance Commission Grant Programs Awarded Amounts Used for Cybersecurity, Fiscal Years 2019 through 2022

Grant program	Description	Total cybersecurity amount identified
Election Security Grant Program	Provides funds for compliance requirements under Section 101 of the Help America Vote Act of 2002 and to improve the administration of elections for federal office, including to enhance technology and make election security improvements.	$153,641,437
Coronavirus Aid, Relief, and Economic Security Grant Program	Provides funds for additional costs and increased activities to prevent, prepare for, and respond to the coronavirus for the 2020 federal election cycle within the parameters of Section 101 of the Help America Vote Act of 2002.	$2,076,390
Total		**$155,717,827**

Source: GAO analysis of Election Assistance Commission grant data and related documentation. I GAO-24-106223

States and U.S. territories funded various cybersecurity activities using EAC's grant programs. For example, using funds awarded from the Election Security Grant Program, one state upgraded election-related computer systems to address vulnerabilities. Another state used the Coronavirus Aid, Relief, and Economic Security Grant Program funds to deploy a software system for secure electronic absentee voting. Other allowable cybersecurity activities under these two grants include, but are not limited to: costs of procuring and maintaining hardware, software, and network infrastructure equipment; threat intelligence and penetration testing; multi-factor authentication systems; network security assessments; fees of managed security service providers; and renewals of security software licenses and subscriptions.

FEMA. FEMA administers five federal grant programs that were used to fund SLTT governments' cybersecurity activities. FEMA reported that the total awarded amount for its five grant programs during fiscal years 2019

through 2022 was $6,805,181,643. Of this amount, about 10 percent (or $669,858,956), was used for cybersecurity-related activities by 50 states, including for cities and counties, six U.S. territories, and 13 Tribal Nations. See table 6 for a list of FEMA's grant programs and total reported awarded amounts for each program, and the amounts that went towards cybersecurity.

Table 6: Federal Emergency Management Agency (FEMA) Grant Programs Awarded Amounts Used for Cybersecurity, Fiscal Years 2019 through 2022

Grant program	Description	Total amount awarded	Total cybersecurity amount identified
Homeland Security Grant Program	Focuses on enhancing the ability of state, local, tribal, and territorial (SLTT) governments to prevent and respond to terrorist attacks. It includes three components: • State Homeland Security Grant Program assists SLTT efforts to prevent and respond to terrorism. • Urban Area Security Initiative assists urban areas to prevent and respond to terrorism. • Operation Stonegarden supports cooperation and coordination among Customs and Border Protection, United States Border Patrol, and SLTT law enforcement agencies to improve border security.	$4,453,518,206	$580,741,091
Transit Security Grant Program	Provides funds to transit agencies to protect critical surface transportation infrastructure and the traveling public from acts of terrorism.	$357,000,000	$33,271,438
Port Security Grant Program	Provides funds to state, local, and private sector maritime partners to support increased port-wide risk management and protect critical surface transportation infrastructure from acts of terrorism, major disasters, and other emergencies.	$400,000,000	$32,618,988
Emergency Management Performance Grant Program	Provides funds to assist SLTT emergency management agencies to implement the National Preparedness System and to support the National Preparedness Goal of the nation.	$1,564,960,511	$15,700,622
Tribal Homeland Security Grant Program	Provides funds directly to eligible Tribes to strengthen their capacities to prevent, prepare for, protect against, and respond to potential terrorist attacks.	$29,702,926	$7,526,817
Total		**$6,805,181,643**	**$669,858,956**

Source: GAO analysis of FEMA grant data and related documentation. I GAO-24-106223

SLTTs used funds from these FEMA programs for a variety of cybersecurity activities. For example, the Homeland Security Grant Program funded upgrades to one entity's outdated network infrastructure. A transit authority used Transit Security Grant Program funds to implement its information security controls for rail operations systems. In addition, Port Security Grant Program funds were used to purchase an

advanced firewall. Further, a recipient of a Tribal Homeland Security Grant Program funded vulnerability scanning software and services.

IMLS. The Institute administers two grant programs that were used to fund SLTT governments' cybersecurity-related activities. IMLS reported that it awarded $708,926 to six states, with some states identifying local libraries, and one city for cybersecurity-related activities from fiscal years 2019 through 2022. See table 7 for a list of these grant programs and the awarded amounts.

Table 7: Institute of Museum and Library Services Grant Programs Awarded Amounts Used for Cybersecurity, Fiscal Years 2019 through 2022

Grant program	Description	Total cybersecurity amount identified
Grants to States Grant Program	Provides financial assistance to develop library services throughout the states and U.S. territories.	$458,926
Museums for America Grant Program	Supports the achievement of championing lifelong learning, strengthening community engagement, and advancing collections stewardship and access.	$250,000
Total		**$708,926**

Source: GAO analysis of Institute of Museum and Library Services grant data and related documentation. I GAO-24-106223

SLTT recipients used funds awarded from these programs for various cybersecurity-related activities. For example, the Grants to States Grant Program funded phishing training and simulations at one entity.[13] In addition, an entity used funds to conduct an audit of its network and cybersecurity practices following a cybersecurity incident that exposed their systems to vulnerabilities. Regarding the Museums for America Grant Program, a grant recipient used funds for cybersecurity training, implementation of a disaster recovery plan, and cloud-based backup systems.

[13]According to the National Institute of Standards and Technology, phishing is a technique to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a website, in which the perpetrator masquerades as a legitimate business or reputable person.

Four Agencies Administered 17 Grant Programs That Were Eligible for Cybersecurity, but Did Not Track Cybersecurity Award Amounts

The cybersecurity-related amounts awarded by the other four agencies in our scope—DOJ, DOL, DOT, and EPA—covering the remaining 17 of the 27 federal grant programs are unknown. Although these agencies track total grants awarded, they reported that they did not track the awarded funding that was used specifically for cybersecurity purposes. According to agency officials, cybersecurity is not the primary purpose of the grants and therefore agencies do not track these amounts.

DOJ. DOJ administers four grant programs that were used to fund SLTT governments' cybersecurity-related activities. DOJ reported that it awarded $1,409,504,294 to entities such as states, cities, and county governments from fiscal years 2019 through 2022; however, the exact amount for cybersecurity-related activities is unknown. See table 8 for a list of DOJ grant programs identified as being eligible to support SLTT governments' cybersecurity enhancements and their descriptions.

Table 8: Department of Justice Grant Programs Eligible for Cybersecurity Expenses

Grant program	Description
Byrne Discretionary Community Project Funding/Byrne Discretionary Grant Program	Provides for improving the functioning of the criminal justice system, preventing or combating juvenile delinquency, and assisting victims of crime.
Edward Byrne Memorial Justice Assistance Grant Program	Provides for hiring additional personnel and/or purchasing equipment, supplies, contractual support, training, technical assistance, and information systems for criminal justice.
National Criminal History Improvement Program	Provides funding to assist states and Tribes with finding ways to make more records available to the National Instant Criminal Background Check System.
Building State Technology Capacity Program	Provides for implementing statewide technology programs to enhance victims' access to services, fostering innovation in the provision of services, improving the quality of services, and improving the accessibility of victim service organizations.

Source: GAO analysis of Department of Justice grant program documentation. I GAO-24-106223

Agency officials stated that DOJ's data are not detailed enough to break out funding for cybersecurity expenses. For example, the Byrne Discretionary Community Project/Byrne Discretionary Grant Program allows funding for network switches, cybersecurity software, and physical

security, such as external cameras. Similarly, grant recipients can use funds from the Edward Byrne Memorial Justice Assistance Grant Program for cybercrime training and to hire cybercrime analysts and investigators.

DOL. DOL provided two funding opportunities to assist states with fraud prevention and overpayment recovery in the Unemployment Insurance program. One of the allowable uses of the grant funds could be for cybersecurity-related activities.[14] DOL reported that it awarded $27,965,619 to entities such as states and U.S. territories from fiscal years 2019 through 2022, but agency officials were unable to determine the amount for cybersecurity activities. See table 9 for a list of DOL's grants identified as being eligible to support SLTT governments' cybersecurity enhancements and their descriptions.

Table 9: Department of Labor Grant Programs Eligible for Cybersecurity Expenses

Grant program	Description
Unemployment Insurance Program Letter 28-20, Change 2	Provides states with funding to assist with efforts to prevent and detect fraud and identity theft and recover fraud overpayments.
Unemployment Insurance Program Letter 22-21	Provides states with funding to support fraud detection and prevention, including identity verification and overpayment recovery activities.

Source: GAO analysis of Department of Labor grant program documentation. I GAO-24-106223

States use funds from these two funding opportunities on integrity-related efforts to prevent fraud, reduce improper payments, and recover overpayments in unemployment programs. In addition to these integrity-related efforts, DOL stated that funding could also be used for cybersecurity-related enhancements, such as technology upgrades to enhance cybersecurity perimeter defense, strengthen identity verification of claimants, and enhance fraud detection and prevention strategies. DOL officials stated that the department does not collect the information that identifies the amounts for cybersecurity-specific activities, but as part of grant reporting, states may identify that they used funds for projects that could include cybersecurity-related activities. For example, one SLTT entity used a portion of the funds to purchase internet protocol address blocking software to block users outside the U.S. from filing online

[14]DOL officials stated that the department provides a variety of funding opportunities that could support cybersecurity activities such as jobs in the industry, which was out of scope for this review.

unemployment claims.[15] Another entity used funds to update its website for added fraud protection.

DOT. DOT administers nine grant programs that may support SLTT governments' cybersecurity activities. They are not required to track data on the cybersecurity-specific activities nor award amounts. See table 10 for a list of DOT's grant programs identified as being eligible to support SLTT governments' cybersecurity enhancements and a description of each.

Table 10: Department of Transportation Grant Programs Eligible for Cybersecurity Expenses

Grant program	Description
Highway Planning and Construction	Assists the states in providing for construction and improvement of highways and bridges. This program also provides for the construction and improvement of highways in the District of Columbia, Puerto Rico, American Samoa, Guam, the Commonwealth of the Northern Mariana Islands, and the U.S. Virgin Islands.
Urbanized Area Formula Grants	Provides federal resources to local and regional government authorities and states for transit capital and operating assistance in urbanized areas and for transportation-related planning.
State of Good Repair Grants Program	Provides capital assistance for replacement and rehabilitation projects for existing fixed guideway systems (including rail, bus rapid transit, and passenger ferries) and high intensity motorbus (buses operating in high-occupancy vehicle lanes) to maintain public transportation systems in a state of good repair.
Formula Grants for Rural Areas and Tribal Transit Program	Provides federal resources to states, local government authorities, and Tribes for transit capital planning projects and operating assistance in rural areas.
State Electronic Crash Data Collection Program	Provides funds to modernize state data collection systems and to enable full electronic data transfer.
University Transportation Centers Program	Provides funds to eligible nonprofit institutions of higher education to establish and operate University Transportation Centers. The objectives of the centers are to advance transportation expertise, provide a critical transportation knowledge base, and address critical workforce needs.

[15]Internet protocol addresses provide a numerical description of the location of networked devices such as computers, routers, and smartphones. These numerical descriptions allow devices to be distinguished from each other over the internet. In some ways, an internet protocol address is like a physical street address.

Grant program	Description
United States Marine Highway Program	Provides funds that expand the use of the nation's navigable waters to relieve landside congestion, reduce air emissions, and generate other public benefits by increasing the efficiency of the surface transportation system.
Port of Guam Improvement Enterprise Program	Provides financial assistance for the planning, design, and construction of projects for the Port of Guam to improve facilities, relieve port congestion, and provide greater access to port facilities.
National Infrastructure Project Assistance	Provides funds to state, local, tribal, and territorial governments for highways, bridges, and freight or passenger rail projects.

Source: GAO analysis of Department of Transportation grant program documentation. I GAO-24-106223

According to a DOT official, these grant programs primarily support the planning and construction of physical infrastructure such as airports, roadways, and bridges, but also may require, as appropriate, that grantees incorporate cybersecurity enhancements in each project. For example, grantees used Highway Planning and Construction funds to implement measures to protect a transportation highway system from cybersecurity threats.

A DOT official added that, although the grants may be eligible to fund cybersecurity-related activities, the department does not collect or monitor cybersecurity-related grant activities and there are no requirements or government standards to do so. Instead, DOT has internal controls designed to track grant expenses related to the nature of the physical infrastructure projects, as discussed later in this report. The official reported that the department awarded over 230,000 grants representing over $270 billion in obligations from fiscal years 2019 through 2022. The official stated that to determine the cybersecurity amounts would require a manual inspection of each awarded grant, which would be resource intensive and time consuming to gather.

EPA. Under the Clean Water Act and the Safe Drinking Water Act, EPA provides capitalization grants to state governments to create and maintain revolving funds, which were used for eligible cybersecurity activities. EPA's revolving fund programs are a federal-state partnership providing financial support for water infrastructure improvement projects, including eligible cybersecurity-related projects. According to EPA officials, set-asides are a type of funding that can be used to administer state drinking water programs, provide technical assistance and training for water

systems, and fund other activities that support achieving the objectives of the Safe Drinking Water Act.[16]

According to an EPA official, a revolving fund functions like a bank in each state that provides low interest loans and other forms of assistance to eligible entities for water infrastructure projects and other eligible activities. Repayments of the loan typically begin 1 year after project completion, with terms up to 40 years for the Drinking Water State Revolving Fund loans and 30 years or useful life for the Clean Water State Revolving Fund loans.[17] See table 11 for details about EPA's two revolving funds.

Table 11: Environmental Protection Agency Grants for Revolving Funds Eligible for Cybersecurity Expenses

Grant program	Description
Capitalization Grants for Drinking Water State Revolving Fund	Provides funds to states and Puerto Rico to establish loan programs that finance drinking water infrastructure improvement projects, including cybersecurity projects. Congress also allowed states to set aside a portion of the revolving fund capitalization grant to support water systems with non-infrastructure needs.
Capitalization Grants for Clean Water State Revolving Fund	Provides funds to states and Puerto Rico to establish a program that offers low interest loans to eligible entities for water quality projects. The revolving fund may be used to develop effective cybersecurity practices and measures at publicly owned wastewater treatment works.

Source: GAO analysis of Environmental Protection Agency grant program documentation. I GAO-24-106223

These programs can be used by states to support certain cybersecurity-related activities such as risk and vulnerability assessments, training, equipment, secure network backups, and threat detection systems. However, an EPA official stated that it would be difficult for EPA to distinguish between cybersecurity-related and non-cybersecurity-related expenses because cybersecurity projects could be a mix of stand-alone projects and those integrated into larger infrastructure projects.

[16]Safe Drinking Water Act, 42 U.S.C. §§ 300f–300j-27.

[17]Useful life is the normal operating life in terms of utility to the owner.

Agencies Established Processes and Procedures to Monitor Cybersecurity-Related Grants; No Cyber-Specific Challenges Identified

Agencies have a variety of processes for monitoring grant programs, including cybersecurity-related grant programs. For each of the agencies that we identified as having cybersecurity-related grant programs, agency officials described one or more grant monitoring processes. For example, officials at agencies in our review said they conduct periodic reviews of progress reports and financial reports submitted by grant recipients.[18] In addition, none of the agencies or organizations representing SLTTs identified challenges with applying for the identified cybersecurity-related grant programs.

All Agencies Established Processes and Procedures to Monitor the Performance of Cybersecurity-Related Grant Program Awards

DOI. DOI provided documentation about its monitoring process that includes reviewing progress and financial reports from grant recipients. In addition, DOI conducts risk assessments prior to awarding grants, and grant program staff may conduct additional inspections. DOI requires grant applicants to disclose whether there is any overlap with other federal grant applications or ongoing federally funded projects.

DOJ. DOJ grant policies include processes to monitor grants by verifying grant project progress in semi-annual progress reports and quarterly financial reports. DOJ policy requires officials to assess grant performance to ensure consistency with program goals, compare grant expenditures to approved budgets, and monitor compliance with grant terms and conditions, including statutory requirements. DOJ also employs a framework to systematically assess risks associated with grants and grant recipients and to determine the level of monitoring needed.

[18]Federal grant-making agencies must use standard, government-wide data elements to collect grant performance information—for example, progress and financial reports—and grant recipients must submit such reports at regular intervals. See 2 CFR § 200.328 and § 200.329.

In addition, DOJ requires applicants to disclose whether they are receiving additional funding which, according to officials, helps reduce duplication of services by federal grant-making agencies. Further, DOJ policy requires that the agency analyze key grant program elements each fiscal year to identify overlap and duplication. According to DOJ policy, some duplication may be allowable and intended—for example, if a recipient uses multiple grants from more than one federal agency to fund related or complementary activities. However, DOJ policy prohibits some forms of duplication, such as a recipient using multiple grants to purchase identical items.

DOL. DOL's grant policy includes monitoring and reviewing quarterly reports from grant recipients to ensure funds are used for permissible activities. The policy also requires that federal staff conduct annual risk assessments and monitoring reviews, such as site visits to measure grant progress, identify areas of compliance, and ensure that federal funds are being used responsibly.

DOT. DOT's grant policy includes steps to review progress and financial reports at least annually. According to officials, DOT also analyzes samples of grant transactions to identify improper payments. According to officials, DOT conducts an additional process review if it identifies a risk in a grant program, such as a state using funds for ineligible projects. Components within DOT, such as the Federal Highway Administration, conduct additional monitoring for the grant programs they oversee—for example, by examining grant recipient reimbursement requests to prevent double billing of costs. DOT allows grant recipients to have multiple funding streams to complete their projects, as long as the same expense is not billed twice, according to officials.

EAC. EAC's grant manual includes processes to review progress and financial reports from grant recipients to ensure recipients are using funds consistent with their stated purpose. In addition, officials said that EAC's inspector general audits the Help America Vote Act grant program funds to identify fraud, waste, and abuse.

EAC officials said they do not prohibit grant recipients from obtaining other federal funds, and they would allow grant recipients to use other federal funds to pay for EAC's matching funds requirement,[19] when

[19]Not all agencies permit this. For example, FEMA does not allow recipients to use its preparedness grant funds to match other federal awards.

permitted by federal regulation.[20] In addition, EAC officials said they maintain awareness of other federal agencies' grant programs—for example, by attending webinars and conferences—in order to share relevant information with stakeholders.

EPA. EPA's grant policy includes processes to conduct annual reviews of grant recipient project performance and annual reviews of recipients' financial and administrative management of grant funds. EPA officials also reported that it reviews project documentation and conducts transaction testing to ensure EPA grants are not funding projects that have already been funded. According to EPA's grant policy, EPA's post-award monitoring processes are designed to ensure effective oversight of grant awards. EPA officials also select a sample of grants each year for advanced monitoring, which are in-depth assessments of recipients' administrative and financial systems, as well as compliance with grant terms and conditions.

FEMA. FEMA's grant manual includes processes to conduct programmatic and financial monitoring to ensure adherence to federal laws, regulations, and grant program requirements. For example, FEMA is required to review quarterly financial reports and biannual progress reports submitted by grant recipients. FEMA officials also reported that it conducts additional monitoring via site visits and in-depth reviews. FEMA's grant manual includes a pre-determined risk criteria that officials use to determine the monitoring needs of individual grants and identify recipients with a high potential for noncompliance.

In addition, similar to DOI, FEMA requires applicants for certain grant programs to disclose whether they will use additional funding to complete their proposed projects.[21] According to officials, FEMA has not identified any instances where Homeland Security Grant Program recipients disclosed or received multiple grant-based funding sources for the same cybersecurity-related projects, and FEMA has not identified any duplication among the grant program recipients.

[20]2 CFR § 200.306(b)(5) (Cost sharing or matching).

[21]Of the grant programs within the scope of this review, FEMA requires applicants for the Port Security Grant Program, Transit Security Grant Program, and Tribal Homeland Security Grant Program to disclose whether they plan to use funding in addition to the FEMA grant to complete proposed projects.

Furthermore, FEMA officials described efforts to coordinate with other agencies with regard to cybersecurity-related grant programs. For example, in FEMA's Port Security Grant Program, Coast Guard officials initially review all grant applications. FEMA officials subsequently conduct an additional review by a panel of subject matter experts to validate the Coast Guard's results and ensure that projects align with the DHS's National Priorities (one of which is cybersecurity). During this process, FEMA may eliminate projects that are deemed to be duplicative.

FEMA also has an intergovernmental review process for coordinating on the grant process with other federal agencies or DHS components. For example, in the Transit Security Grant Program, FEMA typically consults with subject matter experts from DOT, according to officials. In the Homeland Security Grant Program, FEMA officials may send grant applications to subject matter experts at DHS's Cybersecurity and Infrastructure Security Agency for additional review, as needed.

IMLS. IMLS's grant manual includes processes to review progress and financial reports from grant recipients to ensure that expenses are allowable, reasonable, and accurate. In addition, IMLS reported that it reviews grant applications for duplication within and across all applications during each grant program's funding cycle. IMLS grant program officials meet regularly to discuss grant applications and ongoing grant projects, which provides an opportunity to address any potentially duplicative grant activities, according to officials. For IMLS's Library Grants to States grant program, IMLS requires recipients—which are state library administrative agencies—to submit a plan for continuous monitoring of grant performance to ensure compliance with federal regulations. These plans must also describe how recipients intend to coordinate with other agencies within the state to leverage federal grant funds. IMLS officials also conduct site visits every 5 years, according to officials.

Selected Stakeholders, Tribal Nations, and Agencies Did Not Identify Challenges with Cybersecurity-Related Grant Applications

Officials from three national associations representing SLTT governments, two Tribal Nations, and eight agencies did not identify challenges with applying for the identified grant programs that were specific to cybersecurity as a permissible grant activity. However, some officials did identify challenges with the federal grant process in general.

For example, officials from two national associations, one Tribal Nation, and three federal agencies said that the federal grant application process can be cumbersome for applicants—especially when the applicants are small SLTT governments with a relative lack of experience and expertise in grant writing. Another Tribal Nation said it can be difficult to retain staff who have grant writing expertise. In addition, officials from two federal agencies said that grant requirements can be complex for applicants.

As discussed earlier, we have previously reported on a wide range of grant-related issues, including long-standing challenges with federal grant management. In a May 2023 testimony, we provided a summary of common themes covered in these prior reports and testimony related to long-standing challenges with grants management, such as issues with capacity, streamlining, transparency, and internal controls and oversight. For example, our prior work has identified human capital capacity—the extent to which an organization has sufficient staff, knowledge, and technical skills to effectively meet its goals and objectives—as a key factor in successful grants management.

Our prior work has also identified effective oversight as important to providing reasonable assurance that grant recipients use federal grant funds as intended and in accordance with applicable laws and regulations. We have made several recommendations related to grants management in our prior reports—to include recommendations to the Office of Management and Budget and the Department of the Treasury to improve the quality of data on USAspending.gov.[22]

Agency Comments

We requested comments on a draft of this report from DHS, DOI, DOJ, DOL, DOT, EAC, EPA, and IMLS.[23] We received only technical comments from DHS, DOL, DOT, and EPA, which we incorporated as appropriate. DOI, DOJ, EAC, and IMLS stated that they had no comments on the draft report.

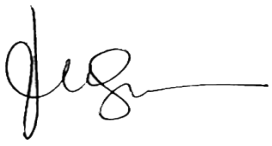
[22]For more information, see GAO, *Grants Management: Observations on Challenges with Access, Use, and Oversight*, GAO-23-106797 (Washington, D.C.: May 2, 2023).

[23]We sent the report to DHS because FEMA is a component of the department.

We are sending copies of this report to appropriate congressional committees; the Departments of Homeland Security, Interior, Labor, Justice, and Transportation; the Election Assistance Commission; the Environmental Protection Agency; the Federal Emergency Management Agency; the Institute of Museum and Library Services; and other interested parties. In addition, this report will be available at no charge on the GAO website at http://www.gao.gov.

If you or your staff members have any questions about this report, please contact David B. Hinchman at (214) 777-5719 or HinchmanD@gao.gov or Tina Won Sherman at (202) 512-8461 or ShermanT@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 I.

David B. Hinchman
Director, Information Technology and Cybersecurity



Tina Won Sherman
Director, Homeland Security and Justice

Appendix I: GAO Contacts and Staff Acknowledgments

GAO Contacts

David B. Hinchman at (214) 777-5719, HinchmanD@gao.gov

Tina Won Sherman at (202) 512-8461, ShermanT@gao.gov

Staff Acknowledgments

In addition to the contacts named above, the following staff made key contributions to this report: Michael Gilmore (Assistant Director), Hugh Paquette (Assistant Director), Kavita Daitnarayan (Analyst in Charge), Amanda Andrade, Christopher Businsky, Rebecca Eyler, Ash Harper, Igor Koshelev, Ahsan Nasar, Ben Nelson, Scott Pettis, Andrew Stavisky, Jason Stonehocker, and Adam Vodraska.

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