GAO

Highlights

Highlights of GAO-25-107313, a report to congressional committees

April 2025

CYBERSECURITY

DHS Implemented a Grant Program to Enable State, Local, Tribal, and Territorial Governments to Improve Security

Why GAO Did This Study

State, local, tribal, and territorial governments provide essential services, including public utilities, healthcare, and public safety. To help address cybersecurity risks and threats to these essential services, DHS implemented a cybersecurity program under the State and Local Cybersecurity Improvement Act.

The act includes a provision in statute for GAO to review DHS's grant program. This report (1) identifies, categorizes, and describes the projects funded by the grant program, (2) examines the extent to which DHS's grant program review process met the requirements of the act, (3) examines the extent to which selected applicants met eligibility requirements, and (4) describes selected state and territory officials' views on the program.

GAO identified and summarized approved cybersecurity projects under the State and Local Cybersecurity Grant Program. GAO analyzed requirements for FEMA and CISA in administering the grant program. GAO also selected a nongeneralizable random sample of seven state and territory grant applicants from various regions of the country to examine the extent to which applicants met eligibility requirements. GAO interviewed selected officials from seven states and two territories who agreed to provide their views on the program.

View GAO-25-107313. For more information, contact David B. Hinchman at hinchmand@gao.gov, or Tina Won Sherman at shermant@gao.gov.

What GAO Found

Pursuant to federal law, the Department of Homeland Security (DHS) implemented a grant program to help state, local, tribal, and territorial governments address cybersecurity risks and threats. As of August 1, 2024, DHS provided about $172 million in grants to 33 states and territories. The grants are funding 839 state and local cybersecurity projects that align with core cybersecurity functions as defined by the National Institute of Standards and Technology (see figure). The projects include developing cybersecurity policy, hiring cybersecurity contractors, upgrading equipment, and implementing multi-factor authentication. Such projects are essential to identifying risks, protecting systems, detecting events, and responding to and recovering from incidents.

Overview of Cybersecurity Project Types Approved for State and Local Cybersecurity Grant Program Funding for Fiscal Years 2022 and 2023

Govern oversight of risk management	**Identify** risk	**Protect** systems from threats and vulnerabilities	**Detect** cybersecurity events	**Respond** to cybersecurity events	**Recover** system operations	**Multiple Categories**
52 Projects	**284 Projects**	**116 Projects**	**43 Projects**	**8 Projects**	**3 Projects**	**333 Projects**
• Policy • Oversight • Workforce	• Risk assessment • Asset management • Upgrade equipment	• Data security • Access control • Training • Authentication	• Monitoring	• Incident response	• Recovery	• Govern • Detect • Identify • Respond • Protect • Recover
Totaling $12M	**Totaling $42M**	**Totaling $20M**	**Totaling $22M**	**Totaling $1M**	**Totaling $256K**	**Totaling $75M**

839 total projects awarded $172,801,312

Sources: GAO analysis of Department of Homeland Security information; tarapong/stock.adobe.com (illustration); Icons-Studio/stock.adobe.com (icons). | GAO-25-107313

In administering the State and Local Cybersecurity Grant Program, DHS's Federal Emergency Management Agency (FEMA) and Cybersecurity and Infrastructure Security Agency (CISA) are responsible for reviewing (1) cybersecurity grant applications and (2) applicants' proposed cybersecurity projects. GAO found that the review and selection processes used by these agencies met the law's specific requirements. For example, CISA used a checklist to validate that applicants' cybersecurity plans contained 16 elements required by the act.

GAO also found that seven selected applicants met the grant program's eligibility requirements, with allowed exceptions. For example, applicants were allowed to submit investment justifications without detailing project-level information if they were not yet ready when the applications were due. In these cases, DHS held awarded funds until applicants addressed requirements.

Selected state and territory officials had positive feedback about the grant program, such as FEMA's willingness to make improvements to the application process. Officials also noted challenges, including sustaining cybersecurity projects after the grant program ends. For example, officials from three states emphasized the importance of reauthorizing the program. However, officials from other states said that they plan to use other federal grant programs or state and local-level funds to continue funding cybersecurity projects.