CENTER FOR DEMOCRACY & TECHNOLOGY

Testimony of Samir Jain
Vice-President of Policy, Center for Democracy & Technology

For the U.S. House of Representatives Committee on Homeland Security
Subcommittee on Cybersecurity and Infrastructure Protection
Hearing Entitled "State and Local Cybersecurity: Escalating Threats, Federal Partnership, and the Resilience of America's Communities"

Thursday, May 21, 2026

Chair Ogles, Ranking Member Ramirez, Chair Garbarino, Ranking Member Thompson, and distinguished Members of the Committee: thank you for the opportunity to testify today on the cybersecurity threats facing state and local governments and the critical role of the federal government in helping to meet them.

My name is Samir Jain, and I am the Vice President of Policy at the Center for Democracy & Technology (CDT), a nonpartisan, nonprofit organization that has worked for more than three decades to advance civil rights and civil liberties in the digital age. CDT brings deep expertise across cybersecurity, privacy, civic technology, elections, and artificial intelligence policy. We engage directly with federal agencies, state and local officials, the private sector, and civil society to promote a more secure and trustworthy digital ecosystem.

State and local governments today are confronting serious cybersecurity threats across nearly every domain in which they operate, from the critical infrastructure that powers our communities and schools, to the systems that administer our elections, to the public benefit programs that millions of Americans rely on for health care, food assistance, and basic income support. When these systems are compromised, people can lose access to critical resources and services at the moments they need them most. Their most sensitive personal information—Social Security numbers, medical records, financial data, immigration status, and information about their children—can be exposed to criminal actors and foreign adversaries, leading to identity theft, financial fraud, harassment, and other harms that can take years to recover from.

A pernicious knock-on effect of these incidents is the erosion of public trust. When Americans see their state DMV, their county hospital, or their child's school district suffer a major breach, their confidence that the government can serve them effectively and handle their personal information with care is shaken. That erosion of trust has consequences far beyond any single incident: it can deter people from enrolling in benefits to which they are entitled, from registering to vote, or from comfortably engaging with public institutions.

These risks are only heightened as artificial intelligence creates new opportunities for malicious actors to attack and exploit government systems at unprecedented speed and scale. The recent announcement of advanced AI systems with substantial cyber capabilities, such as the Mythos Preview from Anthropic, has made clear that the offensive cyber landscape is poised to change dramatically, and small and under-resourced jurisdictions are likely to be particularly vulnerable to that change.

Previously, the federal government has played an indispensable role in helping state, local, tribal, and territorial (SLTT) governments meet these challenges. Through dedicated grant programs such as the State and Local Cybersecurity Grant Program (SLCGP) and through technical assistance from the Cybersecurity and Infrastructure Security Agency (CISA), state and local officials have received targeted funding, threat intelligence, vulnerability assessments, network monitoring tools, tailored guidance, and incident response support. The federal government has offered unique capabilities that no individual state can match: visibility into foreign threat actors and nation-state campaigns; the ability to detect patterns of cyber activity across jurisdictions that no single state could see on its own; and a hub-and-spoke information-sharing architecture, anchored by the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), that has allowed real-time warnings, coordinated defense, and rapid response. Robust investment in cybersecurity and information sharing across federal, state, and local governments over the past decade is a major reason that recent federal election cycles have been secure.

But just as the threat environment is poised to accelerate at an exceptional rate, the federal government has dramatically pulled back. Over the past year, CISA has lost more than a third of its workforce, federal funding for the MS-ISAC and EI-ISAC has been eliminated, key grant programs have been conditioned in ways that effectively block access to cybersecurity support,

and longstanding institutional knowledge and relationships have been lost. The result is a widening gap between rapidly escalating threats and diminished federal capacity to help state and local governments meet them.

My testimony today will make four main points. First, cyber attacks on state and local governments can cause significant real-world harm by exposing sensitive personal information and disrupting critical services. Second, AI is poised to exacerbate the structural challenges that SLTT governments have long faced in defending these systems. Third, the federal government's retreat from its traditional supporting role has already produced concrete harms and threatens to produce many more. Fourth, the federal government should act now to restore funding and capabilities, strengthen information sharing, and reaffirm the shared responsibility that has defined federal–state cybersecurity cooperation.

I. Intrusions into State and Local Government Systems Can Harm People by Exposing Sensitive Personal Information and Disrupting Critical Services.

A. State and Local Governments Hold Vast Amounts of Sensitive Personal Information.

SLTT governments, and the vendors who serve them, hold extraordinary volumes of personal information about Americans. In many respects, this information is even more sensitive than what private companies hold about their consumers. Governments collect this information not because people have chosen to share it in a commercial transaction, but because they must do so to access essential services, exercise their rights, or comply with the law. Key categories of personal data include the following:

1. General Administrative Data and Public Benefits.

States collect a wide variety of personally identifiable information through public benefit and service programs—ranging from Medicaid to SNAP to unemployment insurance.[1] While the specifics vary by state and program, this data routinely includes demographic information such as race, sex, gender, disability status, and citizenship; contact information and home addresses;

[1] See Ctr. for Democracy & Tech., The Leadership Conf. Ctr. for Civil Rights and Tech, & Protect Democracy, *Federal Efforts to Expand Access to Data from State-Run Programs and Individual Privacy* (July 23, 2025), https://cdt.org/wp-content/uploads/2025/07/Federal-Efforts-to-Expand-Access-to-Data-from-State-Run-Programs-and-Individual-Privacy-FINAL.pdf.

records of significant life events including job loss, employment history, marriage, and divorce; medical records and health information; and unique identifying details like Social Security numbers. Taken together, this information offers a comprehensive portrait of a person's family, finances, health, and movements.

2. Voter Data.

Voter registration files are large repositories of personal information collected as a condition of exercising the most fundamental right of citizenship.[2] The precise contents of these files vary across states, but at a minimum they typically include a voter's name, residential address, and identifying details such as full or partial Social Security numbers, driver's license numbers, or state identification numbers.

3. Education Data.

State and local education agencies collect particularly sensitive information about children.[3] Education records can include student demographic information, home addresses, academic performance, disciplinary actions, disability status, health information, and—as CDT has documented in its work on immigrant K-12 students—data points such as place of birth, family demographics, and the number of years a student has attended school in the United States.[4] Because this information concerns minors and is generated in the context of compulsory education, the privacy and security stakes are especially high.

The aggregation of administrative, voter, and education data inside state and local systems means that a successful intrusion at the state or local level can yield a richer, more harmful set of information than a comparable breach in many private-sector contexts.

---

[2] See Ctr. for Democracy & Tech., The Leadership Conf. Ctr. for Civil Rights and Tech, & Protect Democracy, *How Federal Efforts to Access Voter Data Affect Our Privacy, Civil Liberties, and Democracy* (Dec 12, 2025), https://cdt.org/wp-content/uploads/2025/12/How-Federal-Efforts-to-Access-Voter-Data-Affect-Our-Privacy-Civil-Liberties-and-Democracy-final.pdf.

[3] Future of Privacy Forum, *Student Privacy Primer* (Oct. 2021), https://fpf.org/wp-content/uploads/2026/04/2_Student-Privacy-Primer_Final6.pdf.

[4] Kristin Woelfel, *Unique Civil Rights Risks for Immigrant K-12 Students on the AI-Powered Campus, Ctr. for Democracy & Tech.* (Jan. 15, 2025), https://cdt.org/insights/brief-unique-civil-rights-risks-for-immigrant-k-12-students-on-the-ai-powered-campus/.

B. State and Local Governments Face Serious Structural Cybersecurity Challenges.

The sensitivity and concentration of personal data make SLTT systems a natural target for hackers. Unfortunately, state and local governments have also historically faced significant structural challenges in defending against cyber threats, and those challenges are growing more acute.

Many state and local governments face persistent funding and workforce constraints that affect their ability to prepare proactively for attacks and to respond efficiently when those attacks occur. Cybersecurity capabilities vary significantly from one locality to another, depending on leadership, budgets, and organizational capacity. Some agencies have deployed advanced defenses and applied strong cyber-hygiene protocols, while others operate with minimal safeguards, sometimes lacking even basic protections such as multi-factor authentication or regular patching.[5] One survey found that more than half of SLTT agencies were below their target cybersecurity maturity level.[6]

States and local jurisdictions, which often lack the resources to recruit and retain in-house cybersecurity talent, are particularly dependent on federal support and expertise, especially at a moment when many states are confronting serious budget pressures. In a recent national survey, state Chief Information Officers cited insufficient cybersecurity budgets and inadequate cybersecurity staffing as two of the top five barriers to addressing cybersecurity challenges in their states.[7]

These challenges are further compounded by the reliance of state and local governments on third-party contractors that process and handle sensitive data on the government's behalf. The security posture of those contractors is often opaque to the people whose data is at stake and, in many cases, to the officials nominally responsible for oversight. When a major contractor is compromised, the consequences can ripple across many states at once.

---

[5] David Kertai, *Improving State and Local Government Cybersecurity, Info. Tech. & Innovation Found.* (Apr. 27, 2026), https://itif.org/publications/2026/04/27/improving-state-local-government-cybersecurity/.

[6] Multi-State Information and Analysis Center, *Nationwide Cybersecurity Review 2024 Summary Report*, https://learn.cisecurity.org/NCSR-summary-report-2024.

[7] Meredith Ward & Mike Wyatt, *2026 NASCIO-Deloitte Cybersecurity Study* (2026), Deloitte Center for Government Insights, https://www.deloitte.com/us/en/insights/industry/government-public-sector-services/2026-nascio-deloitte-cybersecurity-study.html.

C. Recent Incidents Illustrate the Real-World Harms from Cyber Intrusions.

SLTT governments have suffered a steady stream of breaches and service disruptions with concrete, real-world consequences. Many of these breaches disclosed personally identifiable information of millions of people, exposing them to risks such as identity theft, financial fraud, targeted phishing attacks, and takeover of email or social media accounts. For example, in early 2025, the major government services contractor Conduent—which provides processing support for state benefits programs—suffered a data breach that exposed personal data of more than 25 million people.[8] A major breach at student information system provider PowerSchool leaked personal data for more than 10 million teachers and 60 million students.[9] Earlier this year, the breach of the Canvas learning management platform not only disrupted essential learning activities for schools around the country, but exposed sensitive information of over 275 million users, including private messages that may contain deeply personal communications.[10] The risk to schools is widespread: in CDT's 2025 polling on AI in education, 23 percent of teachers in grades six through twelve reported that their school experienced a large-scale data breach in the 2024–25 school year.[11]

Cyber incidents can also lead to disruption of critical services. Recent local incidents underscore that these are not abstract risks. A ransomware attack in Dallas disrupted a range of systems from emergency dispatch to municipal courts.[12] Several Connecticut local governments were forced to shut down networks in response to a ransomware attack.[13] Foster City, California, saw a range of government services taken offline by a cyber attack.[14] In Winona County, Minnesota, residents

---

[8] Zack Whittaker, *Conduent Data Breach Grows, Affecting at Least 25M People*, TechCrunch (Feb. 24, 2026), https://techcrunch.com/2026/02/24/conduent-data-breach-grows-affecting-at-least-25m-people/.

[9] Briana Mendez-Padilla, *Ransomware attacks in education jump 23% year over year*, K-12 Dive (July 21, 2025), https://www.k12dive.com/news/ransomware-attacks-education-jump-23-percent-h1-2025/753483.

[10] Jason Koebler, *"The Biggest Student Data Privacy Disaster in History": Canvas Hack Shows the Danger of Centralized EdTech*, 404 Media (May 2026), https://www.404media.co/the-biggest-student-data-privacy-disaster-in-history-canvas-hack-shows-the-danger-of-centralized-edtech/.

[11] Elizabeth Laird, Maddy Dwyer & Hannah Quay-de la Vallee, *Hand in Hand: Schools' Embrace of AI Connected to Increased Risks to Students*, Ctr. for Democracy & Tech. (Oct. 8, 2025), https://cdt.org/insights/hand-in-hand-schools-embrace-of-ai-connected-to-increased-risks-to-students/.

[12] Keely Quinlan, *Dallas ransomware attack compromised data of 30,000 people , officials say*, StateScoop (Sept. 25, 2023), https://statescoop.com/dallas-ransomware-attack-cyberattack-data/.

[13] Mary Ellen Godin, *Connecticut Cyber Incidents Highlight Risk for Local Government*, GovTech (Mar. 10, 2026), https://www.govtech.com/security/connecticut-cyber-incidents-highlight-risk-for-local-govt.

[14] Gillian Mohney, *Cyber Attack Continues to Paralyze Foster City, Calif.*, GovTech (Mar. 24, 2026), https://www.govtech.com/security/cyber-attack-continues-to-paralyze-foster-city-calif.

lost access to DMV and vital-statistics services after a ransomware incident.[15] Each of these episodes meant real people unable to renew a driver's license, obtain a birth certificate, or access local services on which they depend.

D. The Public Is Deeply Concerned About the Privacy and Security Risks to Personal Data Held by Government Agencies.

CDT's recent polling confirms that the American public is acutely aware of these risks and is asking for stronger protections. Three in four Americans are concerned about the privacy and security of the personal data that government agencies collect and store about them—a concern that holds steady across demographic groups, regions, and party lines.[16] More than 80 percent of Americans say that having legal protections for the sensitive information that government agencies collect and store about them is important, and 83 percent are specifically concerned that a data breach of a government database could allow their personal data to be misused.[17] As a result of these concerns, 79 percent of Americans agree that Congress should use its authority to hold government agencies accountable when they ignore privacy laws that protect personal data.[18]

II. Artificial Intelligence Is Accelerating the Cybersecurity Risks Facing State and Local Governments.

Cybersecurity threats are intensifying because of the rapid advance of artificial intelligence. AI is a transformative technology with enormous potential benefits, including for cybersecurity defense. But the same capabilities that make AI useful for defenders also make it a powerful tool for attackers, and the offensive threats are evolving more quickly than most state and local governments can adapt.

---

[15] Gavin Michaelson, *Cyber Attack Impacts DMV, Vital Stats in Winona County, Minn.*, GovTech (Apr. 13, 2026), https://www.govtech.com/security/cyber-attack-impacts-dmv-vital-stats-in-winona-county-minn.

[16] Elizabeth Laird, Maddy Dwyer & Quinn Anex-Ries, *Common Concern: Americans Worried About Personal Data Held by Public Agencies and Want Government Accountability*, Ctr. for Democracy & Tech. (Mar. 31, 2026), https://cdt.org/insights/common-concern-americans-worried-about-personal-data-held-by-public-agencies-and-want-government-accountability/.

[17] *Id.*

[18] *Id.*

A. AI Is Lowering the Barrier to Offensive Cyber Operations.

Increasingly capable AI systems are being used to discover and exploit vulnerabilities in software and networks. The recent announcement of the Mythos Preview from Anthropic underscores how rapidly the frontier is shifting. According to Anthropic's own description, advanced models like Mythos can enable users—including those without deep security expertise—to identify and exploit even sophisticated vulnerabilities.[19] The United Kingdom's AI Safety Institute, in its independent evaluation of the Mythos Preview, found that the model was able to execute multi-stage attacks that would otherwise take human operators days, and to discover and exploit vulnerabilities autonomously. The Institute concluded that the model is particularly capable of attacking small, weakly defended, and vulnerable systems where access to a network has been gained.[20] The Institute subsequently found that OpenAI's GPT-5.5 "reaches a similar level of performance on our cyber evaluations."[21]

State and local agencies often operate the small and weakly defended systems that frontier AI models are best positioned to attack. Anthropic shared the Mythos Preview with a limited set of partners through its Glasswing program in an effort to contain its potential impact, though it is unclear whether or how many SLTT governments are currently included in the program.[22] OpenAI has made GPT 5.5 Cyber available through its Trusted Access for Cyber program, which is open to state and local government defenders.[23] But even where SLTT agencies can access advanced models, state and local cybersecurity teams are already stretched thin and may not be in a position to remediate the vulnerabilities they help to identify. Absorbing a surge in newly discoverable vulnerabilities, along with a corresponding spike in active exploitation as these models and capabilities become available to attackers, poses a challenge to all sectors, and SLTT governments may uniquely struggle given their saturated capacity, often limited resources, and heightened targeting.

---

[19] Anthropic, *Mythos Preview*, https://red.anthropic.com/2026/mythos-preview/.

[20] UK AI Safety Inst., *Our Evaluation of Claude Mythos Preview's Cyber Capabilities* (Apr. 13, 2026), https://www.aisi.gov.uk/blog/our-evaluation-of-claude-mythos-previews-cyber-capabilities.

[21] UK AI Safety Inst., *Our Evaluation of OpenAI's GPT-5.5 Cyber Capabilities* (Apr 30, 2026), https://www.aisi.gov.uk/blog/our-evaluation-of-openais-gpt-5-5-cyber-capabilities.

[22] Anthropic, *Glasswing Partner Program*, https://www.anthropic.com/glasswing.

[23] OpenAI, *Cybersecurity in the Intelligence Age* (Apr. 2026), https://cdn.openai.com/pdf/7ca95dce-4424-4b62-9eab-89233bb38f82/oai-cybersecurity-action-plan.pdf.

B. AI Adoption Within Government Introduces Its Own Risks.

SLTT governments are also adopting AI for their own use to build software, interact with constituents through chatbots, and analyze data. Each of these uses can deliver important benefits, but also presents new risks. AI-assisted coding, in which non-expert staff use AI to generate production code, can introduce new security vulnerabilities if not subjected to rigorous review.[24] The use of AI to handle and analyze sensitive information creates additional opportunities for data leakage, including the inadvertent regurgitation of training data, the re-identification of de-identified records, and unauthorized access to data sets used to train or fine-tune models.[25] As governments increasingly deploy chatbots and generative AI tools to allow the public to interact with government agencies, the attack surface grows as those bots are connected to ever more data. It can be extraordinarily difficult to design data flows that prevent AI systems from incorporating sensitive information they have ingested into outputs available to users who would not otherwise have access.[26]

The combination of accelerating offensive capabilities, expanding AI deployment, and limited defensive expertise increases the cybersecurity risks that SLTT governments face.

III. Diminished Federal Support Has Significantly Impeded SLTT Cybersecurity Defenses.

For more than a decade, the federal government has supplied a foundational layer of cybersecurity support to state and local governments. That layer has now been substantially eroded, and the consequences are already visible.

A. What the Federal Government Has Provided.

Federal cybersecurity support for state and local agencies has taken several interlocking forms. CISA has supported SLTT cybersecurity by facilitating information sharing of various kinds; deploying advisors who connect federal and local officials; offering red-team services and

---

[24] Will McCurdy, *Vibe Coding Is Causing 'Thousands' of Data Security Vulnerabilities*, PCMag (May 9, 2026), https://www.pcmag.com/news/vibe-coding-is-causing-thousands-of-data-security-vulnerabilities-says.

[25] Ctr. for Democracy & Tech., *Comments to OMB on Federal Agencies' Use of Commercially Available Information* (Dec. 16, 2024), https://cdt.org/wp-content/uploads/2024/12/CDT-FINAL-Comment-re-OMB-CAI-RFI_December-2024.pdf.

[26] *Id*; Anthony Cuthbertson, *'AI gave me your number': The new trend turning ChatGPT hallucinations into harassment*, The Independent (May 10, 2026), https://www.the-independent.com/tech/ai-doxxing-gemini-hallucination-google-b2973008.html.

incident response support; providing curated feeds of threat intelligence; and funding no-cost cyber defense tools—such as Albert sensors that monitor for network intrusions and malicious-domain blocking tools—that officials have described as irreplaceable.[27] These tools have not only protected election infrastructure; in many counties, they have protected the entire county network, on which hospitals, utilities, courts, and emergency services often depend.[28] For many under-resourced jurisdictions around the country, the cybersecurity assistance that CISA provides has been the only source of network-hardening support available. In Washington State, for example, 15 county governments received endpoint security and malicious-domain blocking tools from CISA that secure their network defenses across the entire county government network.[29]

Information sharing is a critical piece of support the federal government has provided to SLTT governments. Such information includes intelligence about potential threat actors and their objectives, tactics, and likely targets; technical indicators and defensive data such as malicious IP addresses and domains; information about known vulnerabilities that malicious actors could exploit; and practices that can improve resilience. In some cases, the federal government is the only actor that can provide this information. Federal intelligence and security agencies have unique visibility into nation-state and other foreign threats, cross-jurisdictional cyber campaigns, and national patterns which no single state or jurisdiction can see in full.

This information is of particular importance for defending critical infrastructure. U.S. election infrastructure, for example, has been a target of foreign governments, whose attacks have escalated in scale and complexity.[30] During the 2024 election, foreign adversaries targeted state and local elections offices using a variety of techniques, including probes of network defenses,[31]

---

[27] Colin Wood, *Secretaries of State Ask DHS to Retain Essential Election Security Services*, StateScoop (Feb. 24, 2025), https://statescoop.com/secretaries-of-state-ask-dhs-to-retain-essential-election-security-services/.

[28] Tim Harper & Isabel Linzer, *Countdown to the Midterms: Mapping the Rapid Evolution of Election Security*, Ctr. for Democracy & Tech. (Feb. 13, 2026), https://cdt.org/insights/countdown-to-the-midterms-mapping-the-rapid-evolution-of-election-security/.

[29] Wash. Sec'y of State, *Letter on CISA and ISAC Funding* (Feb. 2025), https://www.sos.wa.gov/sites/default/files/2025-02/CISA%20and%20ISAC%20Funding%20Letter.pdf.

[30] Vassilis Ntousas & David Salvo, *Democracy in the Crosshairs: Five Key Trends Driving Foreign Interference in Democracies*, German Marshall Fund (Oct. 10, 2024), https://securingdemocracy.gmfus.org/democracy-in-the-crosshairs-five-key-trends-driving-foreign-interference-in-democracies/.

[31] Microsoft Threat Analysis Ctr., *Russia, Iran, and China Continue Influence Campaigns in Final Weeks Before Election Day 2024* (Oct. 23, 2024), https://www.microsoft.com/en-us/security/security-insider/threat-landscape/russia-iran-and-china-continue-influence-campaigns-in-final-weeks-before-election-day-2024.

distributed denial-of-service (DDoS) attacks,[32] and ransomware.[33] An ineffective cybersecurity information-sharing environment leaves state and local jurisdictions on their own, facing sophisticated nation-state adversaries and criminal organizations without the benefits of collective defense.

Another pillar of federal support has been the Information Sharing and Analysis Center (ISAC) ecosystem. ISACs are non-federal organizations that serve as communities of interest sharing cybersecurity information within a sector. The MS-ISAC, operated by the Center for Internet Security, has long focused on the cyber defense of state, local, tribal, and territorial governments.[34] The EI-ISAC, which was originally established as a pilot within the MS-ISAC after election infrastructure was designated critical infrastructure, has grown to include more than 3,700 state and local election offices and has distributed sophisticated intrusion-detection sensors to more than 1,000 election offices around the country.[35] CISA funded these ISACs through cooperative agreements for many years, recognizing that an ISAC operating independently of the federal government plays a uniquely valuable role: it can serve as a more neutral space, insulated from federal political dynamics, and act as a translator between communities that do not always share the same technical or institutional language.

The Department of Homeland Security has also provided grants to SLTT governments to support cybersecurity efforts. The State and Local Cybersecurity Grant Program (SLCGP) has helped eligible entities address cybersecurity risks and threats to information systems owned or operated by, or on behalf of, SLTT governments.[36] The Homeland Security Grant program has provided states and local governments with support to enhance preparedness against evolving threats,

---

[32] Joao Tome & Jocelyn Woolbright, *Exploring Internet Traffic Shifts and Cyber Attacks During the 2024 U.S. Election*, Cloudflare (Nov. 6, 2024), https://blog.cloudflare.com/exploring-internet-traffic-shifts-and-cyber-attacks-during-the-2024-us-election/.

[33] FBI, Public Service Announcement, *Just So You Know: Ransomware Disruptions during Voting Periods Will Not Impact the Security and Resiliency of Vote Casting or Counting* (Aug. 15, 2024), https://www.ic3.gov/PSA/2024/PSA240815.

[34] Ctr. for Internet Sec., *MS-ISAC Charter*, https://www.cisecurity.org/ms-isac/ms-isac-charter.

[35] Ctr. for Internet Sec., *EI-ISAC 2018 Year in Review*, https://www.cisecurity.org/wp-content/uploads/2019/02/EI-ISAC-2018-YIR.pdf; DHS Off. of Inspector Gen., *DHS Improved Election Infrastructure Security, but Its Role in Countering Disinformation Has Been Reduced*, OIG-24-52 (Sept. 17, 2024), https://www.oig.dhs.gov/sites/default/files/assets/2024-09/OIG-24-52-Sep24.pdf.

[36] CISA, *State and Local Cybersecurity Grant Program*, https://www.cisa.gov/cybergrants/slcgp.

including cybersecurity.[37] These grant programs historically have helped state and local agencies purchase cybersecurity tools, update equipment, and harden networks.

In aggregate, the services and funding provided through CISA and the ISACs have enabled the rapid identification of patterns of cyber behavior affecting or endangering SLTT systems; supported bi-directional information sharing; and provided monitoring, warning, and incident response functions that smaller jurisdictions could never independently sustain. CISA's services have also included access to the .gov top-level domain, made available at no cost to qualifying government organizations—an important defense against impersonation and spoofing.[38]

B. Much of That Federal Support Is Now Gone.

Since last February, CISA has cut more than a third of its workforce[39] and eliminated all funding to the MS-ISAC and EI-ISAC.[40] The rollback of CISA and ISAC resources has further kneecapped state and local agencies' ability to stay on top of emerging threats, proactively safeguard their systems, and effectively respond when cyber incidents occur.

The contrast between 2024 and 2025 is illustrative. In 2024, when more than 100 bomb threats tied to Russian-linked actors targeted polling places nationwide, CISA and the EI-ISAC leveraged intelligence-sharing systems and a real-time operations center to alert officials in advance, helping ensure minimal disruption to voting.[41] In 2025, when bomb threats again targeted polling places—this time in New Jersey on Election Day—CISA issued no public guidance and did not activate its real-time operations center. Election officials were left without the situational awareness that had made such a difference the year before.[42]

---

[37] FEMA, *Homeland Security Grant Program*, https://www.fema.gov/grants/preparedness/homeland-security.

[38] CISA & FBI, *The .gov Domain: Helping Mitigate Election Office Cybersecurity and Impersonation Risks* (Apr. 2024), https://npr.brightspotcdn.com/9c/4e/26fe876d40879b4cb186781b6f13/cisa-fbi-the-gov-domain-helping-mitigate-election-office-cybersecurity-and-impersonation-risks-v2-508c.pdf.

[39] Eric Geller, *CISA Workforce Cut by Nearly One-Third So Far*, Cybersecurity Dive (June 4, 2025), https://www.cybersecuritydive.com/news/cisa-departures-trump-workforce-purge/749796/.

[40] Jessica Lyons, *Feds Cut Funding to Program That Share Cyber Threat Info with Local Governments*, The Register (Sept. 30, 2025), https://www.theregister.com/on-prem/2025/09/30/cisa-kills-agreement-with-nonprofit-that-runs-ms-isac/764252.

[41] Jessica Huseman, Jen Fifield, Hayley Harding, Carter Walker, Natalia Contreras & Alexander Shur, *Election Officials Fear Impact of Trump's Cuts to CISA Cybersecurity Agency*, Votebeat (Feb. 28, 2025), https://www.votebeat.org/2025/02/28/cisa-election-cybersecurity-homeland-kristi-noem/.

[42] Patrick Howell O'Neill, *U.S. Elections Face Security Test as DHS Cuts Local Cyber Support*, Bloomberg (Nov. 3, 2025), https://www.bloomberg.com/news/articles/2025-11-03/us-elections-face-security-test-as-dhs-cuts-local-cyber-support.

The damage is not limited to operational capacity. The federal government, and by extension SLTT partners, have lost years of institutional knowledge and expertise about cyber threat monitoring and response. As Republican Secretary of the Commonwealth of Pennsylvania Al Schmidt has observed, CISA brings "a national and global perspective when it comes to cybersecurity risks and all the rest that each individual state can't do on its own."[43] Removing free access to cyber defenses leaves local governments vulnerable to ransomware and other attacks that affect elections, emergency services, schools, hospitals, and far more.

After the loss of federal funding for the EI-ISAC and MS-ISAC, both organizations have shifted to a paid membership model. They are expected to lose roughly two-thirds of the local, state, territorial, and tribal government members they previously served—precisely the smaller and under-resourced jurisdictions that needed them most.[44] As a result, election officials have lost access to critical information shared across jurisdictions, leaving them less prepared and less able to respond effectively to incidents.

Recent guidance has imposed new conditions on federal grants administered by the Department of Homeland Security, further limiting access to cybersecurity support. The HSGP now requires states to demonstrate compliance with the U.S. Election Assistance Commission's Voluntary Voting System Guidelines 2.0—guidance the Administration has separately sought to use to decertify certain voting machines[45]—and to verify that all poll workers are U.S. citizens through the SAVE system.[46] States unable to meet these new requirements have had their election funds withheld. The SLCGP, for its part, has issued new guidance that prohibits states from using grant funds to participate in the EI-ISAC or MS-ISAC, which CISA has stopped funding directly.[47] As a consequence, some states, including Maine, have refused to accept federal cybersecurity funds altogether rather than comply with the new restrictions, forfeiting roughly $130,000 in additional

---

[43] Jordan Wilkie, *Election Officials in Pa. Sound Alarms over Trump's Cuts to Election Security Agencies*, WESA (Feb. 25, 2025), https://www.wesa.fm/politics-government/2025-02-25/trump-election-security-cuts-pennsylvania.

[44] Eric Geller, *Federal Cuts Force Many State and Local Governments Out of Cyber Collaboration Group*, Cybersecurity Dive (Oct. 1, 2025), https://www.cybersecuritydive.com/news/ms-isac-loses-federal-funding-cyber-impacts/761367/.

[45] Verified Voting, *Executive Order Analysis* (Apr. 2025), https://verifiedvoting.org/blog-executive-order-apr-2025/.

[46] FEMA, *FY25 Homeland Security Grant Program Notice of Funding Opportunity*, https://www.fema.gov/grants/preparedness/homeland-security/fy-25-nofo.

[47] Grants.gov, *State and Local Cybersecurity Grant Program FY25 Guidance*, https://grants.gov/search-results-detail/360215.

cybersecurity support.[48] The combined effect is a system in which states are losing direct federal support, losing the option to use what funding remains to participate in the ISACs that previously filled the gap, and in some cases concluding that the conditions on remaining funds make them not worth accepting.

C. Loss of Trust Between SLTT Officials and the Federal Government.

The federal government's actions over the past year have led to the breakdown in trust with state and local officials, particularly with respect to election cybersecurity. As the federal retreat has deepened, the working relationship between state election officials and Washington has frayed. Some officials have stopped using the cybersecurity services CISA still offers, including physical and cybersecurity assessments, because they fear that information shared during those assessments could later be used to pressure or malign their offices.[49]

A particularly striking example occurred when suspected Iranian-linked hackers targeted systems in Arizona this past summer. State officials chose not to report the incident to CISA, citing distrust in how the agency would handle sensitive vulnerability information.[50] That kind of hesitation can have severe consequences. Ransomware and DDoS attacks against local governments have continued to rise—one recent industry analysis reported a 65 percent surge in ransomware attacks on government agencies in 2025[51]—and during a major incident, every hour that information is not shared can translate directly into expanded harm.

The breakdown in the federal–state cybersecurity relationship will be extremely difficult to repair. Officials have expressed concern that the relationship with CISA built over years of careful and diligent work may be permanently damaged, even if support were to return. That outcome becomes more likely with every additional month of erosion. An earlier draft of the Homeland Security appropriations bill for FY2026 would have earmarked CISA funding to

---

[48] Miles Parks, *Trump's DHS Ties Election Security Grants to Voting Policy*, NPR (Aug. 22, 2025), https://www.npr.org/2025/08/22/nx-s1-5508345/election-security-grants-trump-voting-policy.

[49] Kevin Collier, *Less Staff, Even Less Trust: States Say They Can't Rely on Trump's DHS for Election Security*, NBC News (Aug. 1, 2025), https://www.nbcnews.com/tech/security/less-staff-even-less-trust-states-say-cant-rely-trumps-dhs-election-se-rcna220855.

[50] Derek B. Johnson, *After Website Hack, Arizona Election Officials Unload on Trump's CISA*, CyberScoop (July 21, 2025), https://cyberscoop.com/arizona-secretary-of-state-website-hack-candidate-portal-criticizes-cisa/.

[51] Industrial Cyber, *Comparitech Reports 65% Surge in Ransomware Attacks on Government Agencies in 2025*, https://industrialcyber.co/threats-attacks/comparitech-reports-65-surge-in-ransomware-attacks-on-government-agencies-in-2025/.

rehire ten regional election security advisors and fully funded the EI-ISAC at 2024 levels. A return of that support would be a meaningful first step. But Congress, and CISA, will need to do considerably more to rebuild what has been lost.

IV. Recommended Steps Forward

The federal government plays a unique and important role in supporting state and local cybersecurity for at least three reasons. First, much of the data held by SLTT agencies is collected in response to federal mandates. If the federal government requires SLTTs to collect sensitive information, it bears a corresponding responsibility to help ensure that data is protected. Second, the federal government is uniquely positioned to maximize the value of taxpayer dollars spent on cybersecurity. Cybersecurity is an area in which resource and information sharing produces dramatically better outcomes than independent state-by-state efforts; foundational federal support avoids duplication and improves shared threat awareness. Third, states are increasingly the target of nation-state attacks, which they are ill-equipped to handle given the asymmetry of resources and expertise and which raise national security concerns the federal government alone can fully address.

CDT respectfully urges the Committee to support and pursue the following steps:

A. Restore and Stabilize CISA and ISAC Funding.

Congress should restore funding to CISA and the ISAC ecosystem—particularly the MS-ISAC and EI-ISAC—at levels sufficient to rebuild lost workforce capacity, reactivate suspended programs, and re-establish the free or low-cost services on which thousands of state and local jurisdictions have come to rely. The ISACs deserve particular attention as essential intermediaries during a period when trust in direct CISA engagement has been damaged. As neutral, non-federal entities, ISACs can continue to serve communities that have, at least for now, become reluctant to engage directly with the federal government.

Funding for cybersecurity should also be more stable than it has been historically. Programs that depend on year-to-year uncertainty are difficult to staff and difficult to trust. Multi-year support and durable grant models would foster sustained security programs across SLTT sectors. Information-sharing models in particular require stability to build trust, establish partnerships, and deliver lasting security value. Future funding for SLTT cyber information sharing should

focus on longer-term stability and enduring program-building. These stable funding models are especially beneficial to smaller jurisdictions that have fewer resources and greater difficulty attracting cybersecurity expertise.

B. Reinvigorate the Federal Commitment to Information Sharing.

Congress should expressly reaffirm the federal government's commitment to bidirectional information sharing with state and local governments. That includes restoring the operational capacity at CISA to issue timely public guidance during incidents, activating real-time operations centers during high-risk periods such as elections, and providing SLTT partners with consistent, trustworthy points of contact. Restoring those mechanisms will also require concrete actions to rebuild trust, including clear assurances that information shared with the federal government for defensive purposes will not be repurposed in ways that disadvantage state and local officials.

C. Restore and Maintain Funding to SLTT Governments for Privacy and Cybersecurity Protections.

Particularly in the context of AI-driven vulnerability discovery and exploit development, state and local governments will need ready access to the tools and capabilities that allow them to discover and remediate technical vulnerabilities in their systems. CISA and the MS-ISAC and EI-ISAC previously provided vulnerability scanning, red-teaming, and penetration testing at low or no cost. Restoring those capabilities and ensuring they are extended to state and local governments at scale will be essential to closing vulnerabilities across government networks before they are exploited at speed by AI-enabled adversaries.

Congress should also renew the SLCGP and revisit recent grant-program conditions that effectively block states from using federal cybersecurity dollars to participate in the ISACs or that have led some states to refuse cybersecurity funding altogether. Conditions on federal cybersecurity funds should be designed to maximize the security of state and local systems, not to advance unrelated policy objectives at the expense of cybersecurity.

Conclusion

State and local governments are on the front lines of an evolving cyber threat landscape in which artificial intelligence is increasing the risks. They hold extraordinarily sensitive information about Americans and operate systems on which constituents depend for the most basic functions

of daily life. They face structural resource and workforce constraints that make it impossible for them to meet these threats alone. And they are confronting all of this at precisely the moment when the federal government—the partner on which they have most relied—has dramatically pulled back.

Congress should restore the funding, the programs, and the institutional capacity that have made federal–state cybersecurity cooperation work, while modernizing those tools to address the unique risks posed by advanced AI. It should reaffirm the federal government's commitment to information sharing with SLTT partners, conduct rigorous oversight of agencies whose retrenchment has left systems and data exposed, and ensure that incident reporting and public accountability keep pace with the threats. None of this requires inventing new institutions. It requires renewing the sense of shared responsibility that has defined federal–state cooperation on cybersecurity.

Thank you again for the opportunity to testify. I look forward to your questions.