Ron DeSantis, Florida Governor
Tom Berger, Interim Secretary
Warren Sponholtz, State Chief Information Officer

Testimony of Warren Sponholtz

State Chief Information Officer and Director, Florida Digital Service

State of Florida

Before the U.S. House Committee on Homeland Security

Subcommittee on Cybersecurity and Infrastructure Protection

State and Local Cybersecurity: Escalating Threats, Federal Partnership, and the Resilience of America's Communities

May 21, 2026

Opening Statement

Chairman Ogles, Ranking Member Ramirez, and Members of the Subcommittee: thank you for the opportunity to appear before you today. My name is Warren Sponholtz, and I serve as the Chief Information Officer for the State of Florida and Director of the Florida Digital Service. I appreciate the Subcommittee's attention to the cybersecurity threats facing state, local, tribal, and territorial governments, and to the federal partnerships that help communities defend essential services.

Under Governor DeSantis' leadership, Florida approaches cybersecurity from a simple premise: cyber risk is not just an information technology issue. It is continuity of government, public safety, emergency response, critical infrastructure protection, economic stability, and public trust. The systems we defend support licensing, benefits, elections, law enforcement, education, health, water, transportation, and the many other services Floridians expect to be available every day.

Threat Landscape

The cyber threat picture facing Florida has two faces. The first is financial: criminal groups that steal data, disrupt operations, and demand payment. The second is geopolitical: foreign governments that seek access to the systems Americans rely on so they can steal information, position themselves for future disruption, or weaken confidence in public institutions. Florida sees both, we plan for both, and we do not treat either as theoretical.

Florida is a large and attractive target. We are the third-most populous state in the nation, with roughly 23 million residents. The state enterprise includes 35 state agencies, more than 107,000 employees, and approximately 202,000 devices. State law also gives Florida a role in supporting cybersecurity across nearly 500 counties and municipalities. Florida is home to major military commands, space assets, ports, airports, utilities, hospitals, schools, and public safety networks. An adversary does not look at those responsibilities as separate silos. An adversary sees one target. Our job is to build one coordinated defense.

The threat environment has changed substantially in recent years. Ransomware remains a persistent risk for counties, cities, school districts, Sheriff's offices, utilities, hospitals, and state agencies. These groups are not

always highly sophisticated in the way the public imagines. Often, they use stolen credentials, exploit unpatched internet-facing systems, or rely on social engineering. But their operating model has become highly organized. Ransomware is now an ecosystem: operators, affiliates, brokers, negotiators, data-leak sites, and money-laundering services. Taking down one brand does not end the threat; affiliates can migrate to another platform and continue targeting public services.

At the same time, nation-state activity has become more operationally significant for state and local government. China, Russia, Iran, and North Korea present distinct cyber risks to the United States. Of those, the activity associated with China has changed the conversation most directly for critical infrastructure. Campaigns commonly referred to as Volt Typhoon and Salt Typhoon demonstrate that foreign adversaries are not only seeking data. They are positioning themselves in communications, energy, water, transportation, and other critical sectors in ways that could matter during a future crisis. For Florida, that means our threat intelligence program must look not only for obvious disruption, but also for quiet, long-term access that may be designed to remain undetected for years.

Florida's Coordinated Defense Model

That is why Florida has moved toward a federated but highly orchestrated model of cyber defense. The goal is not to centralize every technology decision. The goal is to create coordination, visibility, speed, and trust across a very large and diverse public-sector environment. State agencies, local governments, educational institutions, law enforcement, emergency management, federal partners, and private-sector critical infrastructure providers each have responsibilities. The state can add value by creating common capabilities, sharing intelligence, coordinating response, and helping smaller entities reach a security baseline they could not afford alone.

Cybersecurity Operations Center

The center of that effort is Florida's Cybersecurity Operations Center, or CSOC, within the Florida Digital Service. The CSOC serves as the state's central threat clearinghouse. It monitors threats across the state enterprise, supports incident response, and helps agencies and partners move from isolated alerting to coordinated detection and response. The CSOC provides incident response assistance to agencies, local governments, and educational institutions. It deploys on-site resources to assist in recoveries and has supported election security in partnership with the Florida Department of Law Enforcement, the Florida Department of State, and the Florida Division of Emergency Management. Maintaining our CSOC has long been a priority for the Governor through his support of recruiting top-tier responders and funding technology enhancements for the important work it handles.

We are also moving the CSOC from a traditional alert-monitoring function toward a more proactive intelligence and analytics operation. That includes advanced analytics for threat hunting, anomaly discovery, behavioral analysis, and enterprise-wide correlation. The objective is straightforward: detect threats earlier, contain them faster, recover more effectively, and maintain government services.

Threat Intelligence and Federal Partnership

Threat intelligence is central to that mission. Florida's intelligence program draws from CISA, federal law enforcement, multistate partners, cybersecurity vendors, managed security providers, proactive threat hunts, incident response activity, and monitoring of criminal marketplaces. But intelligence is only useful when it is operationally relevant. A generic alert about a vulnerability is not enough. Agencies and local partners need timely, contextual information: what is being exploited, where it is likely to matter, what systems may be exposed, what action is expected, and how urgently it must be taken.

Shared telemetry is what makes that possible at scale. When participating entities share security telemetry with the state, Florida can correlate activity across environments. A threat identified in one county, agency, utility, or school system can become a defensive action for others. This is one of the most important benefits of a whole-of-

state approach. It turns separate organizations into a distributed sensor network and allows the state to deliver warnings that are specific, fast, and actionable.

The federal government is an essential partner in this work. Federal intelligence collection and sharing brings national visibility that no individual state can replicate. Federal advisories, threat feeds, automated indicator sharing, vulnerability guidance, and incident coordination help states understand what is happening across the country and what may be heading toward our jurisdictions. Florida adds state and local context to that national view. We understand our agencies, local governments, critical infrastructure operators, emergency management structures, and regional constraints. The best outcomes come when national intelligence and state-level context are combined quickly and operationally.

That partnership has become more important as the threat landscape has changed over the past three years. State and local governments are no longer dealing only with isolated ransomware events or opportunistic criminal activity. We are now defending against a faster, more industrialized criminal ecosystem; increased targeting of schools, utilities, hospitals, and public safety systems; and nation-state activity that is increasingly focused on critical infrastructure and operational disruption.

Enterprise Resilience and Governance

Florida's resilience strategy is broader than any single tool. It includes assessments to identify weaknesses, standards to establish consistent expectations, training to develop cyber skills, remediation support to close known gaps, incident response coordination, and communities of practice that bring security leaders together before an incident occurs. Those relationships matter. During a cyber incident, trust built in advance can reduce confusion, accelerate decision-making, and limit the impact on residents.

Florida has also taken action to reduce risk from applications tied to countries of concern. Governor DeSantis signed legislation enabling prohibited applications to be identified and removed or restricted from government-issued devices, with a defined waiver process for specific mission needs. That is a practical example of governance in action. It is not enough to wait for an incident. We must reduce exposure before applications, vendors, or platforms become operational risk.

Critical Infrastructure Protection

Critical infrastructure is a major focus of Governor DeSantis' strategy. Florida continues to work with critical infrastructure providers to better understand where investment is needed and where systemic risk exists. Through the diligent efforts of the University of South Florida, we have collected useful information from critical infrastructure assessments across the state. We also use the Department of Energy's Cybersecurity Capability Maturity Model to support more consistent discussions about risk, maturity, and priority investments. This is especially important in operational technology environments such as water and wastewater systems, utilities, transportation systems, public safety communications, and industrial control systems. These environments often cannot be secured in the same way as traditional office networks, and many smaller operators lack dedicated cybersecurity staff.

Florida Local Government Cybersecurity Grant Program

Florida's state-funded Local Government Cybersecurity Grant Program is one of our most important tools for reaching local communities. Rather than simply issuing direct payments, the Florida Digital Service procures cybersecurity capabilities on behalf of participating local governments. That model creates economies of scale, reduces procurement friction, gives smaller entities access to enterprise-grade solutions, and helps ensure that deployed tools contribute to a statewide defense architecture. Through Governor's DeSantis' leadership and in partnership with the Florida Legislature, the program has been funded at $30 million, $40 million, and $15 million over the past three funding cycles, respectively.

The capabilities provided through the state program include asset discovery, endpoint detection and response, email security, content delivery network protections, identity and access management, attack-surface management, extended detection and response, and related security operations capabilities. These are foundational controls. Many rural and fiscally constrained communities know they need these protections but cannot obtain them at the scale, speed, or price available through a state-coordinated procurement model. Emphasizing these rural and fiscally constrained communities has been a targeted focus area for Governor DeSantis and the Florida Digital Service.

This program also strengthens statewide visibility. In the current application cycle, Florida received 226 applications, and approximately 90 percent of applicants indicated they were willing to share telemetry with the State CSOC. That willingness is important. It reflects growing trust between the state and local partners, and it enables a more mature defense model in which local investments improve not only the applicant's security, but the security of the broader public-sector ecosystem.

Federal State and Local Cybersecurity Grant Program

The federal State and Local Cybersecurity Grant Program, or SLCGP, complements Florida's state-funded model. In Florida, the federal program is managed through the Florida Division of Emergency Management, with cybersecurity subject matter expertise from the Florida Digital Service. The current focus areas are law enforcement and critical infrastructure, where many needs fall outside the standardized technology bundles provided through the state program. Florida received 66 applications in the current cycle, including applications from 45 cities, 16 counties, and 5 other entities such as water management districts. Fourteen applications were law-enforcement specific.

SLCGP Project Examples

The projects submitted under the federal program illustrate why flexibility matters. One proposed water treatment project would make a high-service pump remote input/output system independent from its main controller, helping the process continue operating during a controller failure or cyber incident. Another project would modernize a city's water and wastewater telemetry system by replacing outdated radio units at a master control site and 35 remote lift stations with more secure and redundant communications. A rural Sheriff's office proposed securing mobile data terminals used by deputies to access dispatch, records, and license plate reader systems in the field. These are not abstract technology upgrades. They are investments in public health, public safety, and continuity of essential services.

The federal program also helps address continuous risk assessment across critical infrastructure and law enforcement environments. One proposed Florida project would provide recurring attack-surface and attack-path analysis for participating critical infrastructure entities and Sheriffs' departments. That type of visibility helps decision-makers understand where vulnerabilities exist, how they could be chained together by an attacker, and which remediation steps would reduce the most risk. For local entities with limited staff, that analytical support can be the difference between guessing and prioritizing.

Another proposed use of SLCGP funding would allow Florida to purchase an enterprise governance, risk, and compliance platform for state agencies. Today, cybersecurity risk information often lives in separate assessments, spreadsheets, plans of action, audit responses, and supporting artifacts. A shared platform would give the state a more consistent way to collect assessment results, score and prioritize cybersecurity risks, track remediation over time, and maintain a catalog of relevant evidence and artifacts. That capability would strengthen enterprise risk governance, improve accountability, support reporting requirements, and help state leaders make better investment decisions across agencies.

Long-Term Federal Partnership and Reauthorization

The SLCGP has helped make that partnership real. It has supported planning, assessments, implementation, and collaboration across the country. It has helped rural communities, small governments, schools, counties, and critical infrastructure operators work on basic cyber hygiene and more advanced resilience needs. It has also encouraged state and local officials to meet before an incident occurs. That may be one of the program's most valuable effects: it creates relationships, governance structures, and shared plans before a crisis.

For those reasons, long-term reauthorization matters. Florida is building long-range cybersecurity plans. The PILLAR Act is complementary to these plans and the direction Florida is already moving. It recognizes the need for sustained federal partnership, supports rural communities, strengthens critical infrastructure and operational technology protections, and accounts for emerging issues such as artificial intelligence and improved intelligence sharing.

At the same time, reauthorization should preserve practical access for the communities that need the program most. High or unstable match requirements can discourage participation, especially among rural and fiscally constrained entities. Reimbursement models can also be difficult for smaller communities that cannot carry large up-front costs. Federal grant design should make it easier for the most vulnerable communities to participate. Additionally, I would be remiss if I did not advise thoughtful caution with AI as it continues to scale into our lives and in these cybersecurity discussions. Disclosure of interactions with AI, protecting minors through parental notification/consent, and safeguarding personal identifying information and sensitive data are all principles we keep in mind in Florida.

Lessons for State and Local Cybersecurity

Florida's experience leads to several lessons. First, shared services work when they are paired with trust and clear governance. Second, telemetry sharing is essential for speed and correlation, but it must be built through partnership, not mandate alone. Third, critical infrastructure protection requires both IT and operational technology expertise. Fourth, smaller governments need procurement support as much as they need funding. Fifth, incident response is strongest when relationships and exercises happen before the emergency.

Cybersecurity as a Sustained Mission

I also want to emphasize that cybersecurity is a sustained operational discipline. It is not a one-time project. New vulnerabilities appear every day. Criminal groups reorganize. Nation-state actors adapt. Local governments replace equipment slowly. Workforce shortages persist. Artificial intelligence will create both defensive opportunities and new risks. The public sector needs funding models, shared services, and governance structures that recognize this as a long-term mission.

Florida has made meaningful progress under the leadership of Governor DeSantis: We have built a central cybersecurity operations capability, expanded incident response support, strengthened state and local collaboration, improved enterprise visibility, reduced costs through shared capabilities, and created grant models that help local governments obtain protections they could not easily acquire alone. But the threat landscape is moving quickly, and we must continue to move with it.

Conclusion

The adversary does not distinguish neatly between a state agency, a small city, a water utility, a school district, a Sheriff's office, or a critical infrastructure provider. To the adversary, those are all pathways into public services and public trust. Our defense must be equally connected. Continued federal partnership and information sharing, sustained support for the SLCGP, and long-term reauthorization through legislation such as the PILLAR Act will help states build that connected defense.

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