State of Utah

SPENCER J. COX
Governor

DEIDRE M. HENDERSON
Lieutenant Governor

Department of Government Operations
Division of Technology Services

MARVIN DODGE
Executive Director

ALAN FULLER
Chief Information Officer

Alan Fuller
Chief Information Officer
Division of Technology Services, State of Utah
NASCIO Secretary-Treasurer

Testimony Before the U.S. House Committee on Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection Hearing on the State and Local Cybersecurity Grant Program

April 1, 2025

Chairman Garbarino, Ranking Member Swalwell, and Members of the Subcommittee:

I am Alan Fuller, Chief Information Officer for the State of Utah, a role to which I was appointed by Governor Cox in March of 2021. As CIO for the State of Utah, I lead the Division of Technology Services, the consolidated IT organization for the executive branch agencies in the state government. As part of my team, I oversee the Cyber Center, which is responsible for defending state IT systems against cyber crime. The Utah Cyber Center (cybercenter.utah.gov) was created to coordinate efforts between state, local, and federal resources to bolster statewide security and help defend against future cyber attacks, by sharing cyber threat intelligence, best practices, and through strategic partnerships.

I am also the Secretary-Treasurer for the National Association of Chief Information Officers (NASCIO.) NASCIO is the collective voice of the nation's state and territorial chief information officers, chief information security officers and chief privacy officers. Its mission is to advance government excellence through trusted collaboration, partnerships and technology leadership. NASCIO is a national leader and advocate for technology policy at all levels of government, and has championed substantial collaboration between states and the federal government to improve cybersecurity preparedness and protect our nation's critical infrastructure.

It is as both CIO for the state of Utah and as a NASCIO officer that I hope to highlight the many successes of the State and Local Cybersecurity Grant Program (SLCGP) today. Though no program is perfect, SLCGP has provided significant support to states and local governments as we have worked to improve our cybersecurity posture and address vulnerabilities.

Utah's Experience

Over the past decade in Utah, state, county, and city governments have witnessed significant escalations in cyber incidents. Initially, attacks were less frequent and sophisticated, often targeting basic vulnerabilities. However, recent years have seen a surge in complex ransomware attacks, data breaches, and phishing campaigns specifically designed to exploit government systems. This evolution reflects a broader trend where malicious actors increasingly target public sector entities, seeking to disrupt services, extort funds, and compromise sensitive data. Local governments, in particular, face challenges in keeping pace with these threats due to budget constraints and limited cybersecurity expertise, making them more susceptible to these evolving cyber risks. Before implementation of the SLCGP, incidents were not reported to the state for fear the state's role would be punitive in nature. If the state was notified, options for response were very limited as either data had already been compromised or system damage, such as ransomware, had already been executed. In many instances, paying a ransom or providing credit monitoring for victims were the only recovery options.

In Utah, we applied for SLCGP funds in 2022 and received approximately $13 million federal funds and $4 million in matching state funds for local cybersecurity efforts. Assessments and audits were conducted to identify any existing cybersecurity issues around the state, including cities, counties, local education agencies, and higher education entities. Results found that cybersecurity systems are significantly under-developed in many cases, leaving local government entities with serious risks (Image 1).

Image 1: Assessment of Cybersecurity Risk for Utah Local Entities

Relative NIST Maturity Level

Low — High

Level in Hierarchy	Control Abbreviation	Control Description	Central Security Services	Entity A	Entity B	Entity C	Entity D	Entity E	Entity F	Entity G	Entity H	Entity I	Entity J	Entity K	Entity L	Entity M	Entity N	Entity O	Entity P	Entity Q	Entity R	Average
Overall			3.62	2.4	2.3	1.6	1.9	2.4	1.3	1.4	1.6	2.2	2.3	2.9	2.4	1.5	1.6	2.0	1.7	2.5	2.4	2.1
Function	ID	IDENTIFY	3.69	2.5	2.0	1.8	2.2	2.7	1.4	1.4	1.3	1.8	2.5	2.9	2.4	1.6	2.1	2.1	1.7	2.3	2.8	2.1
	PR	PROTECT	3.82	3.0	2.3	2.0	2.3	2.8	1.6	1.8	1.9	2.1	2.6	3.1	2.6	1.8	1.9	2.2	1.9	2.6	2.8	2.3
	DE	DETECT	3.60	2.3	3.0	1.6	2.1	2.2	1.3	1.7	2.0	3.0	1.9	3.3	2.5	1.5	1.4	2.0	1.4	2.0	1.9	2.1
	RS	RESPOND	4.18	2.2	2.7	1.4	2.0	2.3	1.1	1.3	1.7	2.8	2.4	3.0	2.4	1.6	1.4	2.2	1.7	2.3	2.0	2.0
	RC	RECOVER	2.83	1.9	1.7	1.3	1.1	1.9	1.1	1.0	1.0	1.2	2.1	2.0	2.1	1.2	1.2	1.7	1.6	3.2	2.6	1.7
Category	ID.AM	Asset Management	4.19	3.1	2.1	1.9	2.9	3.4	1.9	1.7	2.0	2.4	3.0	3.2	2.5	1.5	2.3	2.1	2.0	3.0	3.0	2.5
	ID.BE	Business Environment	3.92	2.4	1.9	1.6	1.9	2.5	1.3	1.2	1.1	1.7	2.7	2.5	2.3	1.5	2.3	2.2	1.5	2.4	3.0	2.0
	ID.GV	Governance	4.20	2.5	2.0	1.7	2.3	2.7	1.4	1.4	1.1	2.0	2.7	3.4	2.3	1.4	2.6	2.4	1.7	2.5	2.8	2.2
	ID.RA	Risk Assessment	3.68	2.6	2.3	1.7	2.3	2.6	1.2	1.7	1.5	2.2	2.3	3.5	2.3	1.7	2.0	2.0	1.6	2.0	2.5	2.1
	ID.RM	Risk Management Strategy	3.77	2.1	1.6	2.0	2.2	2.6	1.2	1.1	1.1	1.2	2.2	3.0	2.4	2.1	2.4	2.1	1.7	2.0	3.1	2.0
	ID.SC	Supply Chain Risk Management	2.37	2.0	1.9	1.8	1.6	2.4	1.1	1.1	1.1	1.1	2.1	1.8	2.8	1.3	1.3	1.8	1.5	2.1	2.4	1.7
	PR.AC	Identity Management, Authentication and Access Control	4.49	3.6	2.6	2.5	2.9	3.0	1.9	2.1	2.5	2.8	2.5	3.3	2.9	2.3	2.2	2.4	2.3	2.8	2.9	2.6
	PR.AT	Awareness and Training	3.68	2.5	3.0	2.2	1.8	3.0	1.3	1.8	1.2	1.5	2.9	3.7	3.2	1.7	1.9	2.3	1.6	3.0	3.3	2.3
	PR.DS	Data Security	3.74	2.8	1.5	1.7	1.7	2.5	1.4	1.7	2.1	1.6	2.4	2.4	2.4	1.5	1.6	1.8	2.0	2.1	2.3	2.0
	PR.IP	Information Protection Processes and Procedures	3.61	2.8	2.2	1.8	2.0	2.6	1.6	1.6	1.7	2.2	2.3	3.2	2.4	1.7	2.1	2.1	2.0	2.5	2.8	2.2
	PR.MA	Maintenance	3.52	3.3	2.3	2.2	3.0	2.9	1.7	2.3	1.8	2.1	3.2	3.3	2.6	2.1	2.0	2.3	2.0	3.1	3.4	2.5
	PR.PT	Protective Technology	3.89	3.2	2.0	1.8	2.4	2.6	1.4	1.6	2.1	2.4	2.5	2.9	2.4	1.7	1.7	2.1	1.7	2.4	2.3	2.2
	DE.AE	Anomalies and Events	3.94	2.2	3.2	1.5	1.9	2.3	1.3	1.7	2.0	3.3	2.2	3.3	2.5	1.3	1.4	2.2	1.4	1.9	1.8	2.1
	DE.CM	Security Continuous Monitoring	3.44	2.7	2.9	1.9	2.2	2.5	1.4	2.1	2.4	2.9	1.7	3.4	2.8	1.8	1.5	2.3	1.6	2.3	2.2	2.2
	DE.DP	Detection Processes	3.43	2.1	2.9	1.5	2.2	1.8	1.2	1.4	1.5	2.8	1.8	3.1	2.3	1.3	1.5	1.7	1.4	1.8	1.6	1.9
	RS.RP	Response Planning	4.92	2.0	2.7	1.2	2.1	2.2	1.0	1.2	2.1	3.0	2.6	2.6	2.5	1.6	1.3	2.3	1.8	2.3	1.8	2.0
	RS.CO	Communications	4.14	2.5	2.9	1.7	1.9	2.6	1.3	1.3	1.7	2.8	2.4	3.2	2.4	1.6	1.6	2.2	1.5	2.4	2.1	2.1
	RS.AN	Analysis	3.70	2.1	2.9	1.5	1.7	2.3	1.1	1.4	1.6	2.9	2.3	3.2	2.2	1.4	1.4	2.2	1.6	2.1	2.0	2.0
	RS.MI	Mitigation	3.81	2.1	2.5	1.5	1.9	2.4	1.0	1.2	1.6	2.3	2.4	3.0	2.3	1.8	1.5	2.2	1.5	1.9	2.1	2.0
	RS.IM	Improvements	4.33	2.3	2.6	1.1	2.3	1.8	1.0	1.1	1.6	2.8	2.4	3.2	2.6	1.4	1.1	2.0	1.9	2.9	2.2	2.0
	RC.RP	Recovery Planning	3.00	2.3	1.7	1.0	1.0	1.7	1.0	1.0	1.0	1.0	2.7	2.3	2.0	1.0	1.0	1.7	1.3	3.7	3.0	1.7
	RC.IM	Improvements	2.42	1.6	1.1	1.1	1.0	1.9	1.0	1.0	1.0	1.0	1.6	1.6	2.3	1.1	1.0	1.4	1.5	3.1	2.5	1.5
	RC.CO	Communications	3.07	1.7	2.3	1.7	1.3	2.2	1.4	1.0	1.0	1.7	1.9	2.1	1.9	1.5	1.6	1.9	2.0	2.9	2.3	1.8

Many of these cities and counties have limited resources with very little to no IT support. They are unable to provide adequate security tools and efforts to protect IT systems. The SLCGP is being utilized to address those concerns by providing much needed tools to local entities.

With funding secured through the SLCGP and corresponding state appropriations, a comprehensive cybersecurity initiative has been deployed across 140 governmental bodies. This encompasses 23 counties, 94 municipalities, and 23 special districts. Consequently, endpoint security has been provisioned for over 26,000 devices, and cybersecurity awareness training, augmented with simulated phishing exercises, is being delivered to 31,000 local government employees. The whole-of-state program incorporates scheduled engagements with local leadership to deliberate on active projects and strategically guide the progression of statewide cybersecurity initiatives.

The results have been extremely positive. We have blocked 7 major cyber attack incidents in the last 6 months. I will speak of two of these.

Shortly before Christmas, the CIO of a local airport urgently contacted me about a cyberattack. Cyber criminals attempted to deploy ransomware on the airport's IT systems, which would have been disastrous, especially during the busy holiday travel season. Our CISO and Cyber Center team immediately worked with the airport's IT team to address the issue. Fortunately, SLCGP funds had provided security tools that were able to detect and interrupt the attack as it was happening. The common tooling and established relationships with local staff enabled a rapid response that limited the impact of the attack. As a result, the airport's service was not interrupted, and no ransom was paid.

Recently, a 911 dispatch center in Utah was the victim of a ransomware attack on systems that provide 911 services. SLCGP funds had provided security tools that detected and interrupted the attack as it was happening. Common tooling and established relationships enabled a rapid response that limited the attack's impact.

A Whole-of-State Approach to Cybersecurity

Utah’s positive experience with this grant program is not an outlier. SLCGP has allowed states to further embrace a “whole-of-state” approach to cybersecurity, which NASCIO defines as collaboration among state agencies and federal agencies, local governments, the National Guard, education (K-12 and higher education), utilities, private companies, healthcare and other sectors to address common technology and cybersecurity challenges. NASCIO has long advocated for a whole-of-state approach to cybersecurity. By approaching cybersecurity as a team sport, information is widely shared and each stakeholder has a clearly defined role to play when an incident occurs.

Under this approach and with the flexibility allowed to provide shared services to local governments, states have been able to use SLCGP to provide vital technology services that many smaller communities otherwise would not be able to implement. While some states have elected to pass SLCGP funding entirely on to local governments, most have either provided

service only or employed a hybrid approach of the two methods. According to one state CIO, "We are implementing (or trying to) a whole-of-state approach, recognizing that our weakest links often need the most support, particularly those under-funded entities that regularly deal with highly sensitive data."

States are also finding a wide array of applicable uses for SLCGP funding. According to the NASCIO 2024 State CIO Survey, cybersecurity training, endpoint detection and assessments are the primary focus for funds, followed closely by support for migration to .gov domains and security monitoring. It is precisely these critically important but attainable basic cyber hygiene measures that the grant was designed to address. Additionally, almost 100% of survey respondents stated that they would like for SLCGP to continue and cited the uncertainty around the program's long-term future as an impediment to further success. As we've seen in Utah, almost every state who has implemented funding from this program has seen some examples of tangible success in improving their cybersecurity posture.

Perhaps most encouraging, however, has been the spirit of collaboration between state and local leaders that the grant has fostered. One requirement to receive funding, the creation of a cybersecurity planning committee to guide how the money will be spent, meaning that these individuals are able to build relationships and trust that will allow them to respond more effectively and successfully to any cybersecurity attacks. Additionally, the "whole-of-state" approach has allowed local governments to learn about state services they can utilize, and for state technology leaders to understand where the greatest needs are.

It is this proven track record of accomplishment that led NASCIO and several other state and local organizations, including the National League of Cities, National Conference of State Legislators and National Governors Association to send a letter to the leaders of the House and Senate Appropriations committees urging them to maintain funding for SLCGP and to refrain from any actions that would undermine its continued success.

Suggested Improvements

Of course, while we are encouraged by the program's accomplishments so far, not everything has been smooth sailing. Initial guidance was slow to be released, and states often received conflicting answers from CISA and FEMA to the same question. However, many of those early issues have been largely resolved.

As Congress begins considering reauthorization of this program, states have the following recommendations:

- Reduce matching contribution for statewide cybersecurity efforts that provide shared services to local governments;
- Stabilize the matching formula across all years of the grant to simplify administration;
- Continue local government assessment requirements for participation;
- Elevate the shared services, whole-of-state option to ensure that states understand that this model is acceptable when administering SLCGP funds;

- Stress that local government cybersecurity assessments and other basic cybersecurity hygiene goals are undertaken before technology purchases are executed;
- Provide long-term stability and assurance for the program with a longer reauthorization.

Conclusion

The State and Local Cybersecurity Grant Program is not a “silver bullet” that can entirely solve our nation’s cybersecurity challenges. It does, however, help stakeholders develop a solid foundation on which to continue to strengthen their defenses and modernize both their technology and processes. I look forward to discussing it today and answering your questions. Thank you.