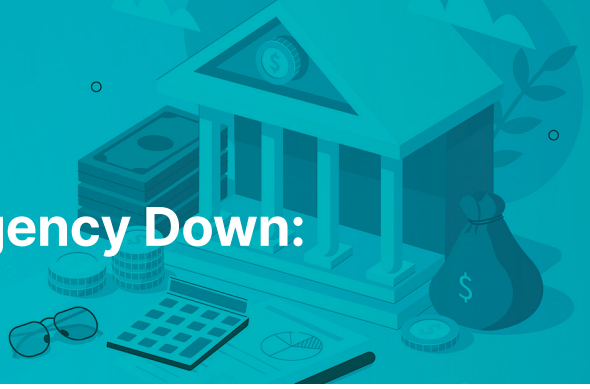
rubrik

Don’t Let Ransomware Take Your Agency Down: How Rubrik and SLCGP Can Help



In recognition of the serious cyber threats facing state and local governments, the US Congress created the State and Local Cybersecurity Grant Program (SLCGP) as part of the 2021 Infrastructure Investments and Jobs Appropriations Act. Launched by the Department of Homeland Security (DHS) but jointly managed by the Cybersecurity and Infrastructure Security Agency (CISA) and Federal Emergency Management Agency (FEMA), SLCGP will give $1 billion in grants over four years to help agencies invest in cybersecurity solutions.

REQUIREMENTS FOR SLCGP FUNDING

In order to qualify and utilize these funds, the program requires state government applicants to establish a Cybersecurity Planning Committee that will develop and approve a Cybersecurity Plan along with local government and education partners. The plan will guide the development of cybersecurity capabilities across the state or territory and must include the adoption of CISA’s best practices for keeping pace with today’s dynamic and increasingly sophisticated cyber threat environment.

HOW RUBRIK HELPS

Rubrik, the Zero Trust Data Security company, is working with state and local governments to fulfill SLCGP requirements with solutions to more effectively secure data from attacks and maintain continuity of critical government services and infrastructure. The following table shows how Rubrik can help your agency meet SLCGP cyber plan requirements.

Cybersecurity Plan Required Elements	How Rubrik Helps
Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.	Rubrik protects your data with a zero trust, natively-immutable filesystem, preventing it from being changed, deleted, or encrypted, so that after an attack, you can trust the existence, integrity and accessibility of the backups.
Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity, including: • Implement multi-factor authentication • Implement enhanced logging • Data encryption for data at rest and in transit • End use of unsupported/end of life software and hardware that are accessible from the internet • Prohibit use of known/fixed/default passwords and credentials • Ensure the ability to reconstitute systems (backups)	Rubrik enables state and local governments to: • Control access to data by implementing multi-factor authentication, temporary one-time password, and role-based access control • Have logically air-gapped backups in an undiscoverable file system with no open protocols to the internet, further protecting your data from bad actors without requiring additional infrastructure at a second site. • Utilize an architecture that isn’t based on Windows OS, and doesn’t rely on open protocols (NFS, SMB) for repositories • Prevent expiration of backups with retention lock that requires at least two admins to delete or expire backups.

Cybersecurity Plan Required Elements	How Rubrik Helps
Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.	Rubrik allows state and local governments to build a logical blueprint to automate the steps, order, and dependencies to recover single files or entire applications. Automated processes allow for frequent testing at scale during "peacetime" and ability to quickly recover critical applications during "wartime."
Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.	Rubrik identifies where sensitive data lies in the organization and it has been exposed, so state and local governments can understand the potential liability of a cyber event. Rubrik also helps identify encryption events and can detect indicators of compromise to prevent the likelihood of reinfection.

GAIN PEACE OF MIND KNOWING YOUR DATA IS FULLY PROTECTED

There's never been a better time to protect your government data from serious and costly cyberattacks. With SLCGP and Rubrik, you can ensure fast recovery of your critical data while staying compliant with CISA best practices for improving cyber defenses and government regulations around citizen data and privacy. Take this opportunity to protect your data before ransomware strikes. Work with Rubrik to see how you can secure your data and keep your agency running, so you can focus on providing the important services that people need.

LEARN MORE

To learn more about the grant program, its qualifications, and how Rubrik can help, go to: https://www.rubrik.com/slgcp.

rubrik

Global HQ
3495 Deer Creek Road
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

op-nam-ps-slcgp / 20230228