

Minnesota IT Services



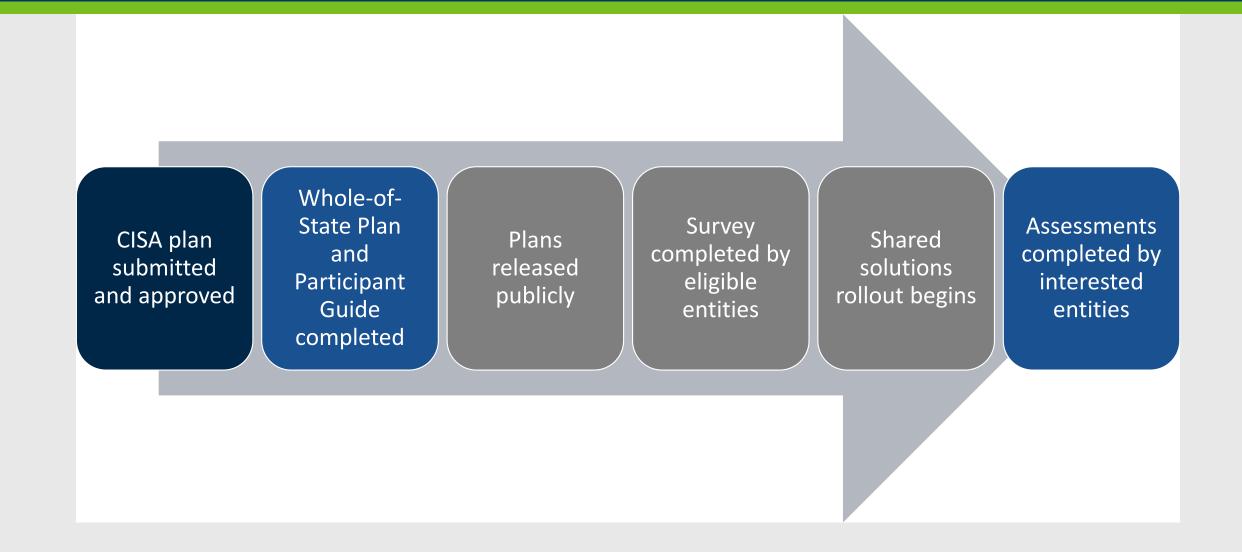
Information Technology for Minnesota Government | mn.gov/mnit





State and Local Cybersecurity Grant Program Update

State and Local Cybersecurity Grant Program Update



SLCGP Program Goals



Mature cyber capabilities – Enable and Enhance Baseline Cybersecurity Capabilities



Reduce risk by leveraging programs -Enhance Adoption of Advanced Cybersecurity Defensive Tools and Capabilities



Collaborate and share information -Expand Threat Intelligence Analysis, Sharing, and Cyber Threat Collaboration throughout Minnesota



Prepare and plan for cyber incidents -Extend Critical Infrastructure Cyber Resiliency

Security Change Items Funding

State, Local, Cybersecurity Grant Program

Cybersecurity Enhancements

MNEIAM Modernization

MNET Security Enhancement

Cybersecurity Funding Objectives

Cybersecurity Programs Enhancements

- Modernize Security Operations Center (SOC)
- Mature enterprise Vendor Risk Management
- Modernize Governance, Risk, and Compliance
- Zero Trust Architecture
- Implement Web Application Firewall (WAF) Service
- Cybersecurity PgM Enhancement Operations

MNET Security Monitoring Enhancement

MNEIAM – CIAM Technology Modernization

Identity, Credential, and Access Management Program



ICAM offers the Executive Branch a vision for organization-wide management and provide a durable, traceable, and transportable digital identity across agencies and over time.

Providing auditability, fraud prevention, and reducing insider threats. These measures help MNIT meet key strategic objectives including elevating Minnesota's digital estate and bolstering successful state cybersecurity efforts.





Emergency Preparedness and MNIT

Information Technology for Minnesota Government | mn.gov/mnit

Advancing Emergency Preparedness in MNIT

- **Goal:** The State of Minnesota must be prepared to sustain and/or restore government and government services in a timely, effective, and safe manner in the event of an emergency or disaster.
- **Role of MNIT:** Partner with agency leadership, Chief Business Technology Officers, and MNIT Enterprise Services to identify, guide, and provide awareness to each agency to ensure continuity for business-critical applications.

Governor's Executive Orders:

- Assigns emergency responsibilities to state agencies
- Creates the Disaster Response and Recovery Council and identifies agency participation
- Provides administrative direction and support for disaster recovery activities

Commissioner's Directive:

- Secure MNIT's IT infrastructure from natural or cyber threats
- Detail roles & work of CBTOs, agency partners, enterprise services: identify and evaluate Priority 1 (P1) applications
- Develop and maintain 24-hour recovery plans for P1 applications

Timeline and Progress on Preparedness

Pre 2019	April 2019 Governor's Executive Order	October 2019 Commissioner's Directive	January 2020 Implementation of Application Portfolio Management	August 2022 Implementation of Disaster Recovery Plan Repository	Future Continuous Improvement & Benchmarking
 Each agency created their own plan, format, and testing schedules Lack of ability to see holistic scope of preparedness and capabilities 	 Orders 19-22 and 19-23 Detailed emergency preparedness planning requirements for agencies Established the Disaster Response and Recovery Council 	 Defined agency and CBTO roles, participation, and expectations regarding disaster recovery Set focus on Priority 1 (P1) applications 	 Inventory and information for applications and component technologies Key to application lifecycle management Current totals 2,694 = Applications 263 = Priority 1 702 = Priority 2 	 Repository and management for disaster recovery plans Current focus on P1 plans 100% of plans are received or in progress 62% of plans are completed and up to date 	 Continued focus on completing and testing P1 applications Integrate tools and data to create efficiencies for ongoing maintenance and updates New technologies and processes that aid mitigation Identify benchmarks and goals used by other institutions

Preparedness: Full Picture



Primary Focus: Mitigation, lessons learned from past emergencies, and identifying new technologies and their impact (cloud computing, teleworking, etc.) can have a big impact on the rest of the areas.



Thank You!