The resources below can help local governments stay up to date on cybersecurity guidelines, best practices, threats, and additional tools.

- **Department of Homeland Security's Cybersecurity and Infrastructure Security Agency** (CISA) — CISA leads the national effort to protect and enhance the resilience of the nation's physical and cyber infrastructure and provides cybersecurity resources and best practices for State, Local, Tribal, and Territorial Governments.
    - StopRansomware.gov — Centralized federal government resources to help public and private organizations understand the ransomware threat, mitigate risk, and know what steps to take in the event of an attack.
    - National Cyber Awareness System Tips — Offers up-to-date information on threats, hoaxes, and safety in plain language for non-technical computer users. You can subscribe to alerts, tips, and updates via the "Subscribe to Alerts" box at the bottom of their webpage.
    - Telework Essentials Toolkit (2020) — Offers best practices and links to resources to help an organization transition to a secure, permanent telework environment by targeting administrators, IT professionals, and everyday telecommuting employees.
- **Center for Internet Security** (CIS) — CIS offers free cybersecurity tools, membership, and services. The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a part of the CIS and is a resource for state, local, and tribal government information sharing, early warnings and alerts, mitigation strategies, training, and exercises.
- **National Institute of Standards and Technology (NIST) Computer Security Resource Center** — The Center provides information security tools and practices, acts as a resource for information security standards and guidelines and identifies key security web resources to support users in industry, government, and academia. It is also a good portal to find all NIST's cyber-related standards.
- **National 911 Program** — This resource hosts information on policies and implementation guides, training opportunities, fact sheets and newsletters, and reports and studies.
- **Water Information Sharing and Analysis Center** (WaterISAC) — WaterISAC is the only all-threats security information source for the water and wastewater sector. Their one-of-a-kind resource serves as a clearinghouse for government and private information that helps WaterISAC members identify risks, prepare for emergencies and secure the nation's critical water infrastructure.
- **SANS Institute OUCH! Newsletters —** OUCH! is the world's leading, free security awareness newsletter designed for everyone. Published every month in multiple languages, each edition is carefully researched and developed by the SANS Security Awareness team, instructors and community members. You can sign up for the OUCH! Newsletter by visiting www.sans.org and choosing 'Newsletters' under Resources.

Cybersecurity plans and procedures are kept confidential by government agencies to further protect their systems. The information below will help local governments devise their own procedures and responses to cyber events and are meant to be a framework for customizing your IS security.

- **Center for Internet Security**
    - CIS Controls V7.1 — A set of basic, foundational, and organizational controls to protect, detect, and respond to cyber incidents for organizations of varying sizes. CIS Controls 17-20 are focused on people and processes, covering security awareness and training; application software security; incident response and management; and penetration tests and red team exercises.
    - Policy Template Guide (2020) — Developed with MS-ISAC, this document offers a series of templates (hyperlinked to download) that can be customized and used as an outline for organizational policies.
- **Cyber Risks to Next Generation 9-1-1** (2019) — Produced by the DHS Office of Emergency Communications, this publication explains the risk landscape, describes the Next Generation 9-1-1 (NG9-1-1) cyber infrastructure, and provides a sample risk assessment plan. Mitigation strategies and response and recovery actions outline potential actions to secure and recover capabilities and services affected in a cybersecurity event. Appendix A is a list of resources for NG9-1-1 administrators and staff.