PARTNERING TO SAFEGUARD **LOCALITIES** FROM CYBERSECURITY THREATS

TOOLKIT

U.S. DEPARTMENT OF HOMELAND SECURITY
CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Municipalities across the United States are at risk of cyber intrusions, with recent incidents demonstrating both potential impacts to critical functions and unauthorized access to sensitive information. The risk is severe, but there are steps that every mayor can take to help safeguard their jurisdiction. This Toolkit provides a summary of steps to make both near-term and enduring progress to maintain the trust that every American places in their local government. The Cybersecurity and Infrastructure Security Agency (CISA), through our regional personnel located across the country, stands ready to work with every municipality in identifying, adopting, and assessing cybersecurity improvements.

Of critical importance, cybersecurity is about culture as much as technology. Many organizations fall into the trap of thinking the Information Technology team alone is responsible for security. As a result, they make common mistakes that increase the odds of a compromise. Culture cannot be delegated. Mayors can play a critical role toward this goal by:

1. **Establishing a culture of security.** Make it a point to talk about cybersecurity to your direct reports and to the entire organization. If you or your senior officials have regular email communications, include updates on security program initiatives. When you set quarterly goals with your leadership team, include meaningful security objectives that are aligned with business goals. Security must be an "every day" activity, not an occasional one. For example, set goals to improve security of your data and accounts through the adoption of multi-factor authentication (MFA) (more on that below), the number of systems you have fully patched, and the number of systems that you backup.
2. **Selecting and supporting a "Security Program Manager."** This person doesn't need to be a security expert or even an IT professional. The Security Program Manager ensures your organization implements all the key elements of a strong cybersecurity program. The manager should report on progress and roadblocks to you and other senior executives at least monthly, or more often in the beginning.
3. **Reviewing and approving the Incident Response Plan (IRP).** The Security Program Manager will create a written IRP for the leadership team to review. The IRP is your action plan before, during, and after a security incident. Give it the attention it deserves in "peace time," and involve leaders from across the organization, not just the security and IT functions. There will be no time to digest and refine it during an incident.

   TIP: Invoke the IRP even when you suspect a false alarm. "Near misses" drive continuous improvements for security programs. Never let a near miss go to waste!

4. **Participating in tabletop exercise drills (TTXs).** The Security Program Manager will host regular attack simulation exercises called tabletop exercises. These exercises will help you and your team build reflexes that you'll need during an incident. Make sure your senior leaders attend and participate.
5. **Supporting the IT leaders.** There are places where the support of the Mayor is critical, especially where the security program needs the help of every staff member. Take ownership of certain efforts instead of asking IT to do so. For example, do not rely on the IT team to persuade busy staff that they must enable a second way to sign-in to their email by enabling MFA. Instead, make the MFA announcement to the staff yourself and keep track of the progress. Personally follow up with people who have not enabled MFA. Doing so creates a culture of security from the top.

In this toolkit, you will find three additional recommendations along with key actions and related resources to help you build, operate, and maintain resilient cybersecurity programs within your locality. The toolkit also shares additional free cybersecurity trainings and resources.

This toolkit is derived from a broader list of tasks called the Cybersecurity Performance Goals (CPG). The work to improve and maintain your cybersecurity posture should be part of a continuous program, not merely a project with a finish line. As you work through the tasks below, CISA recommends that you review all the CPGs and plan to incorporate them into your ongoing security program. See https://www.cisa.gov/cpg for more information.

RECOMMENDATION 1:

INVEST IN THE MOST IMPACTFUL SECURITY MEASURES

AND BUILD TOWARD A MATURE CYBERSECURITY PLAN

Cybersecurity is not one size fits all. Local governments have distinct strengths and weaknesses and a wide range of needs. At the same time, there are relatively simple actions that every organization can take to significantly reduce their cybersecurity risks.

IMPLEMENT HIGHEST PRIORITY SECURITY CONTROLS:

1. Implement multifactor authentication (MFA) (Cybersecurity Performance Goal 1.3)

DESCRIPTION:
MFA is a layered approach to securing online accounts and the data they contain. Even if one factor (such as a user password) becomes compromised, unauthorized users will be unable generally to bypass the second authentication requirement, ultimately stopping them from gaining access to the target accounts.

ACTION:
All local government entities should review CISA's MFA Enhancement Guide, which provides a defined roadmap toward broad MFA adoption. Ensure that all users with elevated privileges, like system administrators, have MFA enabled for all systems.

ADDITIONAL RESOURCES:
- Multifactor Authentication, CISA
- Phishing-Resistant MFA Fact Sheet, CISA

2. Identify and fix known security flaws, prioritizing those that are being actively used by malicious actors (Cybersecurity Performance Goal 5.1)

DESCRIPTION:
While there are many security vulnerabilities in widely used technologies, a small number of these are actually used by malicious actors to compromise victim organizations. By prioritizing these known exploited vulnerabilities, local government organizations can significantly reduce their likelihood of compromise.

ACTION:
Prioritize remediation of vulnerabilities listed in CISA's Known Exploited Vulnerabilities (KEV) Catalog, either by signing up for recurring updates when new vulnerabilities are added or by using a third-party service that automatically identifies the presence of vulnerabilities on the KEV catalog, including but not limited to Palo Alto Networks Cortex, Tenable Nessus, Runecast, Qualys VMDR, Wiz, Rapid7 InsightVM, and Rapid7 Nexpose.

ADDITIONAL RESOURCES:
- Known Exploited Vulnerabilities Catalog, CISA

3. Perform and test backups (Cybersecurity Performance Goal 7.3)

DESCRIPTION:
Implementing, maintaining, and testing backups of critical data is an essential step to reducing impacts from ransomware and other damaging attacks.

ACTION:
Identify data that is critical to continued operations of local government organizations and implement backup solutions that are separated from the operational network. Conduct recurring real-world tests to ensure that data can be readily restored from backups. Where applicable, consider free tools such as Windows Auto-Backup and Google Backup & Sync. As part of the entities' governance program, leaders should request and review evidence of the test restoration tasks and workplans to address any gaps found during the restoration exercise.

ADDITIONAL RESOURCES:
- Data Backup Options

4. Develop and exercise a cyber incident response plan (Cybersecurity Performance Goal 7.2)

DESCRIPTION:
Every local government organization should have an Incident Response Plan that spells out what the organization needs to do before, during, and after an actual or potential security incident. It will include roles and responsibilities for all major activities, and an address book for use should the network be down during an incident. It should be approved by the senior official in the organization and reviewed quarterly, and after every security incident or "near miss".

ACTION:
Develop and regularly exercise a written Incident Response Plan, leveraging CISA's Incident Response Plan Basics two-pager with advice on what to do before, during and after an incident. Additional helpful resources include the State Cybersecurity Best Practices Incident Response Plan.

ADDITIONAL RESOURCES:
- Incident Response Plan (IRP) Basics

IMPLEMENT ADDITIONAL HIGH PRIORITY SECURITY CONTROLS:

1. Minimize exposure to common attacks (Cybersecurity Performance Goals 2.1 and 5.4)

DESCRIPTION:
Malicious cyber actors continuously scan organizations to identify vulnerabilities and execute damaging intrusions. Every local government organization should ensure that their internet-connected assets are up-to-date and free from exploitable conditions.

ACTION:
Enroll in CISA's free Vulnerability Scanning service and quickly address vulnerabilities identified in recurring reports. Take steps outlined by CISA here to reduce the likelihood that a malicious actor can identify the organization's assets when scanning the internet for potential victims.

ADDITIONAL RESOURCES:
- Cyber Hygiene Services, CISA
- Stuff Off Search, CISA

2. Create a training and awareness campaign at all levels (Cybersecurity Performance Goal 4.3)

DESCRIPTION:
All personnel at every local government organization should be formally trained to understand the organization's commitment to security, what tasks they need to perform (like enabling MFA, updating their software and avoiding clicking on suspicious links that could be phishing attacks), and how to escalate suspicious activity.

ACTION:
Review your employee handbook to ensure it has a section on cybersecurity with information on acceptable use of technology, policies, and escalation procedures. Send periodic reminders for staff to review the handbook's security section via email and staff meetings.

ADDITIONAL RESOURCES:
- Cybersecurity Awareness training (amazon.com)
- Security Awareness Training | SANS Security Awareness

3. Prioritize further near-term investments in alignment with the full list of CISA's Cross-Sectors Cybersecurity Performance Goals (CPGs)

DESCRIPTION:
CPGs are a prioritized subset of information technology (IT) and operational technology (OT) cybersecurity practices that all critical infrastructure owners and operators, including local governments, can implement to meaningfully reduce the likelihood and impact of known risks and adversary techniques. They are intended to help establish a common set of fundamental cybersecurity practices that will help organizations of all sizes kickstart their cybersecurity efforts.

ACTION:
Review the CPG website and worksheet, prioritizing goals that the listed as highest impact first. As you develop your monthly, quarterly, and annual roadmaps, include additional CPGs to improve your security posture.

ADDITIONAL RESOURCES:
- Cross-Sector Cybersecurity Performance Goals (CPG)
- CPGs Checklist

4. Over the long-term, develop a unique cybersecurity plan that leverages the NIST Cybersecurity Framework (CSF)

DESCRIPTION:
The CSF is a robust framework for building and maintaining a comprehensive information security program. Governments and enterprises use it to ensure they have covered all the key elements of a mature program.

ACTION:
Organizations should review the CSF as they complete the tasks here, and in the CPGs. Local governments should participate in the free Nationwide Cybersecurity Review (NCSR) 22, which provides metrics that identify gaps and track progress, as well as access to incident reporting and cybersecurity resources.

ADDITIONAL RESOURCES:
- NIST Cybersecurity Framework, especially the Getting Started page

RECOMMENDATION 2:

RECOGNIZE AND ACTIVELY ADDRESS **RESOURCE CONSTRAINTS**

Most local government organizations are doing a lot with a little and resource shortfalls can be a major constraint to implementing effective cybersecurity programs. Local governments should take the following steps to recognize and actively address resource constraints.

1. Work with the state planning committee to leverage the State and Local Cybersecurity Grant Program (SLCGP)

DESCRIPTION:
The SLCGP provides $1 billion over 4 years for a first-of-its-kind grant program specifically for state, local, tribal, and territorial (SLTT) governments funding to support efforts addressing cyber risk to their information systems. The two major first year requirements for this program include the establishment of a Statewide Cybersecurity Planning Committee and the development, by this committee, of a Statewide Cybersecurity Plan.

ACTION:
Review the resources below and coordinate with your Statewide Cybersecurity Planning Committee on applying to the program.

ADDITIONAL RESOURCES:
- FY22 State and Local Cybersecurity Grant Program Fact Sheet, CISA
- State and Local Cybersecurity Grant Program Frequently Asked Questions, CISA
- Homeland Security Grant Program, FEMA
- Homeland Security Grant Program (HSGP) Application Process, FEMA

2. Utilize free or low-cost services to make near-term improvements when resources are scarce

DESCRIPTION:
As part of our continuing mission to reduce cybersecurity risk across U.S. critical infrastructure partners and SLTT governments, CISA has compiled a list of free cybersecurity tools and services to help organizations further advance their security capabilities. This living repository includes cybersecurity services provided by CISA, widely used open-source tools, and free tools and services offered by private and public sector organizations across the cybersecurity community. CISA will implement a process for organizations to submit additional free tools and services for inclusion on this list in the future.

ACTION:
Evaluate your security program's need for services and tools to determine if any in this catalog are a fit for your needs.

ADDITIONAL RESOURCES:
- Free Cybersecurity Services and Tools, CISA

3. Ask more of technology providers

DESCRIPTION:
Local governments should expect the technology used for core government functions to have strong security controls enabled by default for no additional charge.

ACTION:
During the technology procurement and renewal process, ensure that vendors do not charge more for security features like MFA and logs. Be especially aware of the "SSO tax", the practice of changing customers more to connect a service (like a financial or time keeping system) to the organization's Single Sign On (SSO) portal. Further, as you deploy products be sure to review the product's "hardening guide". A hardening guide is a set of steps to make the product less dangerous. As you become aware of upcharges for security features, or unsafe defaults, start a dialog with ISAC members to assess a strategy for working together with the vendor to remediate. CISA is ready to serve as an advocate for the local government community in advancing technology products that are fit for purpose to support our nation's critical government systems. Where a local government organization identifies a technology that is not meeting expectations for security built-in, contact your regional cybersecurity advisor to begin a conversation on how we can help.

ADDITIONAL RESOURCES:
- Cyber Security Advisors, CISA

4. Minimize the burden of on-premise security

DESCRIPTION:
Many local government organizations operate their own IT systems, known as "on premises" systems. Such systems require time to patch, to monitor, and to respond to potential security events. Few organizations have the resources and expertise to keep them in the cloud.

ACTION:
Local government organizations should urgently consider migrating on-premises IT services to the cloud. While it is not possible to categorically state that "the cloud is more secure," migration to the cloud will be a more secure and resilient option for many organizations. Consider first cloud versions of your user identity system, and your mail system. Talk to your CISA regional representative for guidance on secure cloud migration.

ADDITIONAL RESOURCES:
- Google Workspace | Business Apps & Collaboration Tools
- Azure Active Directory | Microsoft Azure
- Microsoft 365 - Subscription for Office Apps | Microsoft 365

RECOMMENDATION 3:

FOCUS ON COLLABORATION AND **INFORMATION SHARING**

Local government entities struggle to fund cybersecurity resources while combating continuous threats. Situational awareness into changes in the risk environment is critical to ensure that resources are allocated to the most effective security mitigations and controls. Localities should take the following steps.

DESCRIPTION:
By focusing on collaboration and information sharing, organizations can stay aware of critical alerts on current threads and vulnerabilities.

ACTION:
Join cybersecurity collaboration groups, such as the MS-ISAC. MS-ISAC membership includes reporting as well as data and information sharing. In addition, MS-ISAC members receive critical alerts on current threats, risks, and vulnerabilities; free cyber tools, resources, and services; and 24/7 access to assistance that includes threat incident analysis, mitigation, and remediation.

Join MS-ISAC—Free for U.S. State, Local, Tribal & Territorial Government Entities, Center for Internet Security (CIS)

ACTION:
Build a strong and enduring relationship with CISA and FBI regional cybersecurity personnel. Report every cyber incident to CISA, every time.

- Regional Offices
- Report to CISA, CISA
- Internet Crime Complaint Center (IC3), FBI

Note: *This toolkit is not comprehensive. CISA applies neutral principles and criteria to add items and maintains sole and unreviewable discretion over the determination of items included. CISA does not attest to the suitability or effectiveness of these services and tools for any particular use case. CISA does not endorse any commercial product or service. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by CISA.*