Massachusetts Municipal Cybersecurity Roadmap

The Massachusetts Municipal Cybersecurity Roadmap provides municipalities with a path to creating strong, robust cybersecurity cultures and programs, with services, resources, and guidance. The Minimum Baseline of Cybersecurity is a framework to help municipalities improve their cybersecurity posture, and the basis for the Massachusetts Municipal Cybersecurity Roadmap.

For municipalities, technology offers the opportunity to make citizens' lives less stressful by providing easy ways to pay tax bills and parking tickets, and efficient ways for municipalities to issue permits and other services. With today's enhanced technologies, however, the threat of a cyber attack on municipal systems is ever-increasing, and the path to implement a cyber program is often unclear and overwhelming.

The Minimum Baseline is made up of four goals:

TRAINED AND CYBER-SECURE EMPLOYEES

To reduce the risk of cybersecurity incidents by improving the training and awareness of system users.

IMPROVED THREAT SHARING

To respond faster to threats and improve regional awareness and resilience by sharing cyber threat information.

CYBER INCIDENT RESPONSE PLANNING

To strengthen municipal defenses and minimize cyber incident impacts by creating an effective strategy for handling cyber incidents.

SECURE TECHNOLOGY ENVIRONMENT AND BEST PRACTICES

To reduce the threat of cybersecurity incidents and minimize incident impacts by implementing some basic best practices to make your technology.

The Commonwealth designed the Massachusetts Municipal Cybersecurity Roadmap to help municipalities improve their cyber posture by creating best practices to enable municipalities to:

1. Identify where they are in relation to the four goals of the Minimum Baseline of Cybersecurity, and
2. Plan the next steps for their cybersecurity journey.

Massachusetts Municipal Cybersecurity Roadmap

How to Use:

The Roadmap chart identifies recommended no- and low-cost federal and state programs and resources to help municipalities increase their cyber resiliency, based on their cyber maturity. Most of these no- or low-cost offerings provide guidance and resources to help municipalities implement programs.

- The Four Minimum Baseline of Cybersecurity Goals are identified in the left column of the Roadmap
- The Levels of Maturity are Identified in the Top Row

LEVEL 1 Foundational – for municipalities starting their cybersecurity journey, entry-level offerings to begin

LEVEL 2 Intermediate – for municipalities with a foundational level of cybersecurity, offerings to build a stronger IT environment

LEVEL 3 Advanced – for municipalities with more advanced cybersecurity programs, risk-based programs to stay ahead of evolving threats

LEVEL X Optimal – for municipalities with a healthy, mature-cyber posture where risk is regularly evaluated and CISA's Cybersecurity Performance Goals (CPGs) are used to prioritize investment in a limited number of essential actions with high-impact security outcomes

<u>How to determine your organizations location and recommended next steps on the Roadmap</u>

1. Identify the programs your municipality currently has in place or is implementing:
   a) Circle any programs you have or are implementing in Levels 1 through 3.

Highlight your recommended next steps:

a) If you don't have any of the programs in the Level 1 – Foundational column, you are at the start of your journey and should implement the Level 1 – Foundational programs first.

b) If you have a program circled, look to the next maturity level of the Minimum Baseline goal and identify programs to implement next. Note that you may be in Level 1 for one Minimum Baseline goal and Level 2 for another—it's okay to have programs in different goals.

c) To implement a robust, holistic cybersecurity program, municipalities should implement programs for each Minimum Baseline goal.

Massachusetts Municipal Cybersecurity Roadmap

Minimum Baseline Goal	**LEVEL 1** Foundational	**LEVEL 2** Intermediate	**LEVEL 3** Advanced	**LEVEL X** Optimal
TRAINED AND CYBER-SECURE EMPLOYEES	Execute a cybersecurity awareness training program for all employees	Implement a yearly employee cyber-awareness training	Require employee year-long cybersecurity awareness training annually Institute role-based cybersecurity training/certifications for IT Staff	• All employees participate in year-long cyber awareness training annually • IT & Cybersecurity staff are trained, equipped, and certified on technologies to safeguard and mitigate their environments from cyberattacks.
IMPROVED THREAT SHARING	Register for Cyber Information and Alerts from trusted sources EOTSS, CISA, MS-ISAC, Comm Fusion Center	Join MS-ISAC Collaborate with Regional IT Groups for information sharing, discuss cyber threats/challenges, participate in CRMWG/RITD Quarterly Meetings	Consistently collaborate amongst municipalities and schools on cybersecurity strategies & implementation	• Organization is active in collaboration • IT and Cybersecurity employees receive the latest threat alerts and are members of information-sharing groups in order to mitigate the risk of attack.
CYBER INCIDENT RESPONSE PLANNING	Policy for Incident Reporting	Complete Asset Inventory Identify & document recovery response for capital named in Asset Inventory	Establish a team to complete a written cyber incident response plan, test, update & print out	• An IR Plan defines steps for incident preparation, analysis, containment, eradication, and post-incident. A recovery plan is in place. Plans are printed out and easy to locate. • All employees know who to call and what to do in case of an incident.
SECURE TECHNOLOGY ENVIRONMENT AND BEST PRACTICES	Migrate to Dotgov (.gov) domain Implement Multi-Factor Authentication (MFA) and End-Point Detection and Response (EDR)	Determine your organizations cyber posture through Vulnerability Scans Implement plan to improve cyber posture & put mitigations & best practices in place	Implement Minimum Baseline of Information Technology for best practices Join a SOC for continuous monitoring	• Risks to business environment are identified & proactively monitored via protective technologies • Monitoring program established to detect threats in real time.Response times and impacts of incidents are monitored and minimized • Recovery times and incident impacts are monitored & minimized

Massachusetts Municipal Cybersecurity Roadmap

LEVEL 1: FOUNDATIONAL

Municipalities beginning their cybersecurity journey are advised to follow these Foundational steps as they begin to develop a path to a cybersecurity program.

1. Implement a cybersecurity awareness training program for all employees. EOTSS offers a no-cost Municipal Cybersecurity Awareness Grant Program annually.
2. Register for and review threat-sharing information from trusted sources.
3. Identify your organization's process to record cyber incidents and the information that needs to be gathered.

Resources:

- The Executive Office of Technology Services & Security (EOTSS) offers a free Municipal Cybersecurity Awareness Grant Program annually.
- Massachusetts Interlocal Insurance Association (MIIA) offers MIIA CyberNET® an online e-learning platform that MIIA members can use to train their community on cybersecurity best practices.
- Register for Cyber Information and/or notifications from trusted sources:
  - EOTSS Cybersecurity Awareness Bulletins
  - Cybersecurity Infrastructure Security Agency (CISA) #Stop Ransomware tips and guidance AND Phishing Guidance: Stopping the Attack Cycle at Phase One
  - Join the Massachusetts State Police/Fusion Center Cybersecurity Program MCP Membership Signup Link which routinely distributes cybersecurity intelligence products, sitational awarenss and other cyber-intelligence informatin to stakeholders.
  - Subscribe to Center for Internet Security's (CIS) Multi-State Information Sharing and Analysis Center (MS-ISAC) and additional sector specific ISAC's E-ISAC (municipal electric), Water ISAC (municipal water), EI-ISAC (Elections Infrastructure for City/Town Clerks) and IT-ISAC (information technology)
- Utilize existing municipally focused cyber toolkits, such as those available through the Mass Cyber Center to get you started.
- Create a notification tree for a Cyber Incident; including who/what to report, print out for IT/Leadership:
  - Inform your organizational Leadership, City/Town Counsel, Police Department, and your Cyber Insurance Provider. If you are insured by MIIA, please call 800-526-6442.
  - Notify EOTSS SOC Center via email eotss-soc@mass.gov or (508) 820-2233
  - Report the Incident to CISA using this form
  - Depending on the incident type, you may be required to report to the Massachusetts Attorney General's Office or the Office of the Comptroller

Massachusetts Municipal Cybersecurity Roadmap

LEVEL 2: INTERMEDIATE

Assess your municipality's cybersecurity posture, establish processes, and implement technology to create an INTERMEDIATE maturity level and build on your foundational security posture to strengthen your IT environment.

1. Require annual employee cyber-awareness; incentives may assist with this endeavor.
2. Collaborate with Regional IT Director (RITD) Groups ; get to know your neighboring municipalities, communities, and resources. Leverage ways for information sharing, discuss cyberthreats/challenges, and participate in CRMWG/RITD Quarterly Meetings. Request to join here
3. Assess your municipality's cyber posture and identify process and technology gaps. This enables you to identify key areas of improvement and implement best practices to better protect the organization and its data from cyber threats.

Resources:

- Apply for EOTSS/OMST Cybersecurity Health Check or CISA's CyberHygiene (CyHy) Vulnerability Scan, results facilitate your ability to create a plan, prioritize, and budget accordingly to mitigate vulnerabilities.
- Community Compact Cabinet (CCC) Grants – Opportunities for funding in the areas of Information Technology Best Practice Grants, IT Grants, Municipal Fiber Grants, or Efficiency & Regionalization Grants
- ITS78 Statewide Contract for Data, Cybersecurity, and Related Audit, Compliance, and Incident Responses Services
  ITS78 contains state-approved vendors who specialize in cybersecurity-related activities such as gap analysis, best practices, data loss prevention, risk assessments, penetration testing, Incident Response Planning (IRP), managed threat detection and response, and forensic investigations.
- State & Local Cybersecurity Grant Program (SLCGP) Participate in the municipal cybersecurity awareness training grant program, role-based IT cybersecurity training, establish IT policies & procedures and best practices, implement Multi-Factor Authentication (MFA) and End-Point Detection and Response (EDR). Implement a plan to improve cyber posture & put mitigations & best practices in place.
- Conduct an Asset Inventory that includes all devices. (to know what you are trying to protect and how). ITS75 Statewide Contract for Software & Services may be used to procure a software product that scans environments for assets, and a vendor may be able to provide complimentary services under ITS75. The ITC73 Statewide Contract for IT Hardware & Services could be used for inventorying physical IT assets. ITS74 Statewide Contract for Project Services could be used for procuring services only related to inventorying software and IT assets
- Protecting our Future Partnering to Safeguard K-12 Organizations from Cybersecurity Threats
- Join MS-ISAC at no cost and gain access to the programs listed in their MS-ISAC Services Guide

Massachusetts Municipal Cybersecurity Roadmap

LEVEL 3: ADVANCED

For municipalities who have implemented and maintained a foundational baseline of cybersecurity, it is important to ADVANCE to the next steps to further protect data, networks, and applications in a consistent, risk-based manner. Take ownership of your IT infrastructure and prevent risk.

1. Continue to require and participate in annual employee cyber-awareness training.
2. Implement role-based IT and Cybersecurity training for the technology workforce and seek certifications to develop knowledge and contribute to retention.
3. Actively collaborate with other municipalities on cybersecurity strategies & implementation
4. Implement best practices such as password policy, disaster recovery technology/process, firewall minimum best practices, domain name system (DNS) standardization, and more…
5. Write a Cyber Incident Response Plan (IRP)
6. Have stakeholders in your cyber–Incident Response Plan (IRP) participate in Tabletop Exercises (TTX) that test the accuracy and steps to respond.
7. Consider joining a Security Operations Center (SOC) to Monitor, Detect, and Respond that would be responsible for protecting your organization against cyber threats. Round-the-clock monitoring of your network and investigation and response to any potential security incidents.

Resources:

- CISA's *Incident Response and Awareness Training* for IT Workforce
- Cyber Resilient Massachusetts Working Group's Minimum Baseline of IT
- Cyber Incident Response Planning: Using the Asset Inventory as a guide, identify how you will respond and recover if an incident impacts one or more devices and/or systems within your IT infrastructure. Mass Cyber Center's Cyber Incident Response Planning Materials includes an IRP template, and CISA's Cybersecurity Tabletop Exercise Tips and Incident Response Plan (IRP) Basics and will provide you with some insight to write, review, and test your plan
- Mass Cyber Center, in it's Cyber Incident Response Planning Materials, includes TTX's and CISA offers a Cybersecurity Scenarios and Insider Threat Mitigation TTX 's
- Institute role-based cybersecurity training/certifications for IT staff. CyberTrust Massachusetts is transforming cyber education and training statewide, by introducing hands-on, experiential learning environments. Vendors on the ITS78: Statewide Contract for Data, Cybersecurity, and Related Audit, Compliance, and Incident Responses Services may also provide educational opportunities.

Massachusetts Municipal Cybersecurity Roadmap

LEVEL X: OPTIMAL

Level X represents a healthy, mature-cyber posture where municipalities regularly evaluate risk and use CISA's Cybersecurity Performance Goals (CPGs) to prioritize investment in a limited number of essential actions with high-impact security outcomes. The CPGs align with the NIST Functions:

CPG 1 - Identify: Develop an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
CPG 2 - Protect: Develop and implement the appropriate safeguards to ensure delivery of services.
CPG 3 - Detect: Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
CPG 4 - Respond: Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
CPG 5 - Recover: Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that we impaired due to a cybersecurity event.

1. Trained and Cyber-Secure Employees **(CPG 1, CPG 2)**
   - All employees participate in annual cyber awareness training.
   - IT & Cybersecurity staff are trained, equipped, and certified on technologies to safeguard and mitigate their environments from cyberattacks.
2. Improved Threat Sharing **(CPG 3)**
   - Organization is active in collaboration activities.
   - IT and Cybersecurity employees receive the latest threat alerts and are members of information-sharing groups in order to mitigate the risk of attack.
3. Cyber Incident Response Planning **(CPG 4, CPG 5)**
   - An IR Plan defines steps for incident preparation, analysis, containment, eradication, and post-incident. A recovery plan is in place. Plans are printed out and easy to locate.
   - All employees know who to call and what to do in case of an incident.
4. Secure Technology Environment and Best Practices (CPG 2, CPG 3)
   - Risks to business environment are identified & proactively monitored via protective technologies
   - Monitoring program established to detect threats in real time. Response times and impacts of incidents are monitored and minimized
   - Recovery times and incident impacts are monitored & minimized

Resources:

- More information on the CPG's can be found here.