Interview Guide

Reference:
https://masscybercenter.org/why-cybersecurity/municipal-cybersecurity/municipal-cybersecurity-toolkit/minimum-baseline

Introduction: Project Description and Consent

Project description:

The Massachusetts Cyber Center (MassCyber) and researchers from the MIT Cybersecurity Clinic are conducting a series of interviews of IT and cybersecurity professionals in municipalities across Massachusetts. The goal of the interviews are to gauge knowledge and understanding of MassCyber's Minimum Baseline of Cybersecurity for Municipalities recommendations among Massachusetts municipalities IT professionals, and to learn what challenges municipalities may be facing in implementing the Minimum Baseline.

Who we are:
The MIT Cybersecurity Clinic is an organization directed by Professor Lawrence Susskind, in the MIT Department of Urban Studies and Planning. The goal of the organization is to provide education around defenses against social-engineering based cyberattacks, and to help conduct cybersecurity vulnerability assessments for municipalities.
The MassCyberCenter is an Massachusetts state agency whose "mission is to enhance conditions for economic growth through outreach to the cybersecurity ecosystem of Massachusetts, while fostering cybersecurity resiliency within the Commonwealth."

Verbal Consent
This interview is voluntary. You have the right not to answer any question, and to stop the interview at any time or for any reason. We expect that the interview will take about 30 to 45 minutes.

• Unless you give us permission to use your name, title, and / or quote you in any publications that may result from this research, the information you tell us will be confidential.

• We would like to record this interview so that we can use it for reference while proceeding with this study. We will not record this interview without your permission. If you do grant permission for this conversation to be recorded, you have the right to revoke recording permission and/or end the interview at any time.

This project will be completed by January of 2022. All interview recordings will be stored in a secure work space and anonymized if requested.

Any information that is obtained in connection with this study and that can be identified with you will remain confidential and will be disclosed only with your permission or as required by law.

In addition, your information may be reviewed by authorized MIT representatives to ensure compliance with MIT policies and procedures.

I understand the procedures described above. My questions have been answered to my satisfaction, and I agree to participate in this study. I have been given a copy of this form.

Please state all that apply

[] I give permission for this interview to be recorded.

I give permission for the following information to be included in publications resulting from this study

[] my name   [] my title   [] anonymized direct quotes from this interview

Section 0: General Questions

1. Name?
2. Organization and Role?
3. How long have you been working…
 3.1. in this role?
 3.2. in this organization?
 3.3. in your field?
4. At the present, how would you describe your organization's cybersecurity readiness?
5. If applicable, what are the main projects or tasks you have undertaken regarding cybersecurity in your organization?

Section I: General Inquiries

1. Do you communicate regularly with other cities or towns with regards to cybersecurity?

   1.1. How do you communicate or share information with those cities and/or towns?

2. Have you ever been the target of a cyberattack? If so, could you describe to us what you experienced and how did you resolve it?

Section II: MassCyberCenter, Municipal Cybersecurity Toolkit, and Minimum Baseline of Cybersecurity for Municipalities

1. Are you familiar with The Massachusetts Cybersecurity Center or MassCyberCenter for short?
  1.1. Can you describe briefly what MassCyberCenter does?

2. Are you familiar with the Municipal Cybersecurity Toolkit?
  2.1. Have you ever used the resources available in the Municipal Cybersecurity Toolkit?

3. If you have used the Municipal Cybersecurity Toolkit:
  3.1. In what way was the Municipal Cybersecurity Toolkit helpful to you?
  3.2. In what way was the Municipal Cybersecurity Toolkit not especially helpful?

4. Are you aware of the Minimum Baseline of Cybersecurity for Municipalities?

<u>Section III: Goal 1 (Trained and Cyber-secure Employees)</u>

1. Do you understand Goal 1 (Trained and Cyber-secure Employees)?
2. What are concrete ways in which your organization is meeting this goal? (e.g., specific practices)? How well equipped do you feel in meeting this goal?
3. What are difficulties you face and/or foresee with regards to reaching this goal?
4. Do you think the resources and guidance provided are helpful for achieving this goal?
5. What are other resources that the state or other government could provide that would be helpful in this regard?
6. What are your thoughts with regards to this goal?

Section IV: Goal 2 (Improved Threat Sharing)

1. Do you understand Goal 2 (Improved Threat Sharing)?
2. What are concrete ways in which your organization is meeting this goal? (e.g., specific practices)? How well equipped do you feel in meeting this goal?
3. What are difficulties you face and/or foresee with regards to reaching this goal?
4. Do you think the resources and guidance provided are helpful for achieving this goal?
5. What are other resources that the state or other government could provide that could be helpful in this regard?
6. What are your thoughts with regards to this goal?

Section V: Goal 3 (Cyber Incident Response Planning)

1. Do you understand Goal 3 (Cyber Incident Response Planning)?
2. What are concrete ways in which your organization is meeting this goal? (e.g., specific practices)? How well equipped do you feel in meeting this goal?
3. What are difficulties you face and/or foresee with regards to reaching this goal?
4. Do you think the resources and guidance provided are helpful for achieving this goal?
5. What are other resources that the state or other government could provide that could be helpful in this regard?
6. What are your thoughts with regards to this goal?

Section VI: Goal 4 (Secure Technology Environment and Best Practices)

1. Do you understand Goal 4 (Secure Technology Environment and Best Practices)?
2. What are concrete ways in which your organization is meeting this goal? (e.g., specific practices)? How well equipped do you feel in meeting this goal?
3. What are difficulties you face and/or foresee with regards to reaching this goal?
4. Do you think the resources and guidance provided are helpful for achieving this goal?
5. What are other resources that the state or other government could provide that could be helpful in this regard?
6. What are your thoughts with regards to this goal?

Section VII: Closing Questions

1. Now that you've seen these goals and resources, how likely would you say that you are to use this toolkit in the future? What are reasons why you would or would not?
2. What other resources do you use to stay current with trends in cybersecurity?
3. What additional resources would you like to have available with regards to cybersecurity in Massachusetts?
    3.1. Can you describe them very briefly?