C3 VOLUNTARY PROGRAM

State, Local, Tribal, and Territorial (SLTT) Government Leadership Agenda

As a State, Local, Tribal of Territorial (SLTT) government leader, you recognize that cybersecurity is critical to any organization, no matter how small. But given the scope and complexity of the issue – and in the face of resource constraints – how do you start a conversation with your leadership team about how to best address your organizations' needs?

Below are suggested questions and topics you can use to help guide a conversation about your organization's current cybersecurity posture and best practices. This agenda can also assist you in starting a conversation about how to use the National Institute of Standards and Technology's (NIST) Cybersecurity Framework as a guide for your cybersecurity procedures and policies.

1. Overview of Cyber Threat

Consider providing a threat briefing to update your team on the current cyber threat environment, especially as it pertains to SLTT governments. The Multi-State Information Sharing and Analysis Center (MS-ISAC) can provide context, if needed.

2. Understanding Risk

Facilitate a discussion about how your organization uses information technology (IT) to support your core organizational culture and functions, how you allocate and support cybersecurity resources, and how you maintain and improve your state of preparedness.

Questions about Our Organization

1) What does our organization value?
2) How will our agency or our stakeholders be affected if we are unable to perform our key functions due to a cyber incident, such as a data breach or denial of service?
3) What are our most valuable information assets? How are we protecting them? What adversaries might want to access or damage these assets?
4) What are potential confidentiality, integrity, or availability impacts to information important to our stakeholders if a cyber incident were to occur?
5) Do we collect and/or store sensitive personally identifiable information (PII), law enforcement sensitive, and/or health data? If so, how is it collected, protected, stored, and destroyed?
6) Do we have the budget to adequately manage our agency's cybersecurity risk?

Questions about Our Resources

1) Do we have the proper staffing and resources to protect our information and cyber infrastructure? If not,
    a. What resources are we able to allocate toward improving our internal capabilities?
    b. What external services can we access or organizations can we partner with to secure these capabilities?
2) How are decisions made for cybersecurity and resource allocation?
3) How are we informed about relevant trends and new technologies?
4) How are risks communicated across the organization?
5) Is our leadership team regularly informed about the level of cyber risk to our organization?
6) What is our plan to recruit, train, and retain our cybersecurity workforce? What cybersecurity skillsets are lacking across our agency?
7) What awareness efforts are we conducting with our employees (e.g. training)?

Questions about Our Preparedness

1) What is our agency's plan to manage cybersecurity risks, including insider threats?
2) Have we projected the incidents we will face, based on trends and threat analysis?
3) Do we have robust incident response plans in place to quickly manage a cyber incident? How often are they

exercised, tested, and updated?

4) What are the biggest challenges our organization faces in responding to and minimizing the impact of cybersecurity incidents?
5) How do we work with the Multi-State Information Sharing and Analysis Center (MS-ISAC) and National Cybersecurity and Communications Integration Center (NCCIC) to share information on threats, vulnerabilities, and incidents?
6) How do we interact with other government agencies to share information and best practices?
7) To what extent has our organization been able to meet the security objectives and responsibilities outlined in FISMA or regulatory requirements?
8) What is our status in implementing government-wide cybersecurity programs based on accepted frameworks and standards such as the NIST Cybersecurity Framework?
9) Do we have contract oversight mechanisms in place to protect sensitive data or key systems from compromise in a contractor network?

3. Existing Organizational Security Plans

Discuss the state of existing organizational security plans with your leadership team.

1) When did we first develop our plans, and when did we last update them?
2) Do our plans address cyber risk management and physical risk management?
3) Who should review the plan(s), both internally and externally?
4) How will we communicate the information in the plan(s) to our employees to ensure compliance?
5) Do our plans address the questions in the sections above?

4. Next Steps for Our Organization

Discuss next steps for your organization based on your current cybersecurity posture.

1) Which are high priority areas for immediate action?
2) Will we revise our short, medium, and long-term security goals based on our current cybersecurity posture?
3) How often will the leadership team meet to discuss cybersecurity?

5. Discussion of Government Resources

Discuss which cyber risk management resources would be beneficial to your organization.

- **Visit the Critical Infrastructure Cyber Community (C^3, pronounced "CCubed") Voluntary Program website** for a list of cybersecurity and risk management tools and resources geared specifically toward SLTT Governments: www.us-cert.gov/ccubedvp/getting-started-sltt.
  - Resources include a growing list of State and local government cybersecurity websites, which may contain information and resources specific to your geographical area.