APPENDIX A

Prepare for a Cyber Disruption - Steps to Take

1) **Identify your cyber response team.**

   Clarify who the key players are, outline roles and responsibilities, and clearly identify which individuals have the authority to take critical response actions. Document how to contact team members 24/7, designate an alternate for key roles, and outline a cadence for how and when the team will convene and deliver updates.

   First Response Team: Includes the Cyber Response Manager and other IT/OT security staff to investigate an incident.

   Cyber Response Steering Committee: Typically includes business executive leadership, CIO or senior IT management, information security officer, and Legal Counsel (or their designees) to confirm a cyber incident/disruption and oversee response.

   Full Cyber Response Team: A complete list of individuals and roles that can be engaged as needed to scale-up and support response such as 1) internal: Public Information Officers, Human Resources, Financial Officer, and Emergency Manager and 2) external: other government cyber response organizations, cyber insurance and law enforcement.

2) **Identify contacts and response service contracts for cybersecurity service providers and equipment vendors.**

   Keep an updated list of vendor contacts and the support they can provide if a vulnerability is identified in vendor equipment. Identify a contact person for the Internet Service Provider (ISP). If incident investigation, forensic analysis, or other forms of incident response support, is contracted out to a third party, identify the contact person, determine the process for engaging their support, and identify the person on the Cyber Response Team who is authorized to engage their services. Determine the expected response timelines for each partner.

3) **Understand systems and environment.**

   Document where system maps, logs, and inventories are kept and maintained (both online and hard copy), along with the person(s) who has the credentials to access them. Document access credentials and procedures for removing access or providing temporary access to cyber responders.

4) **Outline reporting requirements and timelines.**

   Depending on the type or severity of cyber incident/disruption, there may be requirements to report to regulatory agencies and local/state/federal officials, often within the first 24 hours, and sometimes as little as 6 hours. Determine your legal and contractual obligations to report incidents/disruptions to federal/state/local officials, insurance providers, and other third parties.

5) **Identify response procedures.**

   Document procedures for investigation and documentation, containment actions for various types of attacks, and procedures for cleaning and restoring systems. Identify and pre-position the resources needed to preserve evidence, make digital images of affected systems, and conduct a forensic analysis, either internally or with the assistance of a third-party expert.

   Identify the external response organizations—including law enforcement, information sharing organizations, and cyber mutual assistance groups—that might engage during cyber incident response, particularly for when resources and capabilities are exceeded.

   Identify key contacts within external response organizations and build personal relationships in advance. Determine how much information to share and when. Document who has the authority to engage these organizations and at what point they should be notified.

6) **Develop strategic communication procedures .**

   Identify the key internal and external communications stakeholders, what information to communicate and when, and what situations warrant internal communication with employees and public communication with citizens and the media. Develop key messages and notification templates in advance.

7) **Define legal team response.**

   Cyber response should be planned, coordinated, and executed under the guidance of the legal team. Procedures to promptly alert the legal team of a cyber incident/disruption need to be in place. To ensure compliance and preserve the legal posture, the legal team should be directly involved with the investigation, documentation, and reporting.

8) **Exercise and train staff.**

   Staff should be trained on cyber response processes and procedures regularly. Cyber response exercises or participation in industry exercises should be conducted frequently to test cyber response preparedness.