PREPARING FOR A CYBER INCIDENT

CYBERSECURITY ASSESSMENT TOOL

To prepare for threats posed by cyber intrusions, complete this brief assessment to quantify your organizations' level of cybersecurity and identify areas for improvement.

Section 1: Pre-Incident			
Are you prepared?		**Yes**	**No**
Cyber Benchmarking Does your organization have a vision of what a successful cybersecurity program entails and a comprehensive plan to achieve this vision?	Establishing a vision for success is necessary to measure progress, which may help justify funding in the future. Without clear, achievable tasks that support the accomplishment of larger programmatic goals, progress may stagnate if employees feel overwhelmed. Breaking tasks down into manageable pieces encourages sustained achievements.		
Operational Organization Does your organization have an operational structure that includes a clear chain of command in handling cyber incidents?	Effective management depends, in part, on maintaining a small span of control and a clear reporting structure, particularly in cyber incidents where event ownership is not always readily apparent.		
Jurisdictional Hazard Identification Has your jurisdiction identified cybersecurity as a hazard in operational plans?	Identifying cyber hazards in context of a risk assessment illuminate preparedness activities that help anticipate an incident. Providing a description of cyber threats as part of internal policies or employee resources will increase awareness of cybersecurity protocols and reduce the risk of intrusions or attacks.		
Continuity of Operations Does your organization have a Continuity of Operations or Business Continuity Plan that considers cyber incidents?	A cyber incident may disrupt an agency's ability to carry out their mission essential functions, and the infrastructure your organization relies on might not be there. Organizations need to consider how they resume and recovery from these complex incidents.		
Consequence Management Does your organization have a plan to manage both the virtual and physical results of a cyber incident?	Cyber incidents can have cascading impacts across an organization that are difficult to manage, unless plans address both spheres of consequence management.		
Alert Notification Has your organization considered how to alert staff and the public of a cyber incident if communications are down?	Cyber intrusions can target or disrupt conventional methods of communication and information-sharing. Internal and external alert notifications can pose critical challenges during a cyber incident.		
Penetration Testing Does your organization know which cyber threats pose the greatest risk to your virtual systems?	Testing for security weaknesses is essential to addressing those vulnerabilities and becoming more prepared for cyber disruptions.		
System Hardening Does your organization have cybersecurity measures to make it less vulnerable to cyberattacks?	Protecting systems through virtual hardening mechanisms such as patching, scanning, and log monitoring is a critical aspect of overall cybersecurity and keeping your organization safe.		

Section 2: Incident Response

Are you prepared?		Yes	No
Threat Identification Does your organization train on spotting suspicious activity?	Training and testing employees to know what to look for as suspicious virtual activity and what to do about it can help prevent cyber incidents from occurring.		
Multi-Year Training and Exercising Does your organization have a long-term plan for delivering training and exercises to improve cybersecurity capabilities?	Having a long-term plan in place to provide consistent training and exercises will help ensure that an organization continues to improve cyber-related skillsets.		
Operational Coordination Does your organization have relationships and points of contact for relevant response partners?	Relationship building, particularly with nontraditional agencies and organizations, before an incident occurs can facilitate a smoother response and recovery from a cyber emergency.		
Cyber Response Has your organization trained staff on what to do if a cyber incident occurs?	Cyber incidents tend to get worse every moment action does not occur. A workforce trained to be proactive during a cyber incident makes for an active approach to cybersecurity and response.		
Reputation Management Is your organization prepared to respond to cyber incidents in a manner that safeguards assets and reputation?	Understand the assets you aim to protect and why. Identifying potential vulnerabilities and determining an appropriate response in advance is crucial to mitigating the effects of a cyber incident, which can help save face later on.		
Cyber Reporting Does your organization know who to report cyber incidents and intrusions to?	Reporting cyber incidents and intrusion is an important aspect of cyber response that helps prevent their recurrence.		

Section 3: Post-Incident

Are you prepared?		Yes	No
Restoration of Services Does your organization have checklists, job aids, or other reference documents to facilitate post-incident assessments?	Certain aspects of cyber intrusions may be difficult to detect. Providing standardized tools, and ensure employees are familiar with these tools, will minimize potential oversight of dormant or surviving cyber threats.		
After-Action Reporting Does your organization have a process for convening a review of the incident with relevant leadership or employees?	A critical aspect of learning from cyber incidents requires understanding the cause or vulnerabilities that existed prior to the incident. After-action reporting addresses this gap by identifying areas for improvement and an improvement plan.		
Mitigation Activities Does your organization identify steps to prevent future attacks?	Completion of mitigation projects may reduce vulnerability to cyber incidents or their effects. Mitigation projects may include applying software patches, replacing or repairing infrastructure, or creating or updating internal policies once an organization's vulnerabilities have been exposed.		
Funding Recovery Has your organization identified potential funding streams to pay for recovery and to implement mitigation projects?	Lack of funding may significantly reduce an organization's ability to recovery from a cyber incident. With that said, A comprehensive mitigation plan is worthless unless your organization has the financial means to act on it and implement the specified projects.		

Other Considerations: