

CISA AND CYBERSECURITY PLANNING

Mark Breunig

Cybersecurity State Coordinator, Region 10 (Alaska)

November 7, 2023



CISA Mission and Vision

Mission: Lead the National effort to understand and manage cyber and physical risk to our critical infrastructure






Vision: Secure and resilient critical infrastructure for the American people

DEFEND TODAY. SECURE TOMORROW.



Critical Infrastructure Sectors

KEY ACTIVITIES:

-  **IDENTIFY AND VERIFY SUSPICIOUS CYBER ACTIVITY**
-  **UNDERSTAND INCIDENTS AND VULNERABILITIES**
-  **BUILD AND MAINTAIN PARTNERSHIPS**
-  **SHARE TIMELY AND ACTIONABLE INFORMATION**
-  **COLLABORATE WITH PARTNERS TO MITIGATE RISK**

16 CRITICAL INFRASTRUCTURE SECTORS:



CISA Touchpoints

Cybersecurity Advisors (CSC/CSAs)

- Assesses and advises on cybersecurity threats

Protective Security Advisors (PSAs)

- Assesses and advises on physical threats

CISA Central

- CISA's SOC monitoring all threats
- Provides HQ support for regions
- Hosts the Cyber Resource Hub



CISA Cybersecurity No Cost Offerings

CISA Cybersecurity Regional Advisors

Preparedness Activities

- Information/Threat Indicator Sharing
- Cybersecurity Training, Workshops, Tabletops
- Cyber Exercises and “Playbooks” Review
- National Cyber Awareness System (US-CERT)
- Incident Management Workshops
- Ransomware Guide / Playbook
- **Cybersecurity Assessment Services**
 - Cyber Performance Goals (**CPG**)
 - Cyber Resilience Essentials (**CRE**)
 - External Dependency Management (**EDM**)
 - Cyber Infrastructure Surveys (**C-IST**)
 - Cyber Security Evaluation Tool (**CSET**)

Delivered by CISA HQ Vulnerability Mgt Team

- Phishing Campaign Assessment (**PCA**)
- Cyber Hygiene Scanning (**CyHy**)
- Web Application Scanning (**WAS**)
- Remote Penetration Testing (**RPT**)
- Risk & Vulnerability Assessment (**RVA**)

CISA HQ Response Assistance

- Remote / On-Site Assistance
- Malware Analysis
- Hunt and Incident Response Teams
- Incident Coordination

State Based Protective Security Advisors

- Physical Security Assessments
- Incident liaisons between government and private sector for CI protection



Cybersecurity Plan the Why:

An organization needs a cybersecurity plan to:

- Help prevent costly business disruptions
- Minimize damage and reduce recovery time by providing clear guidelines for employees to follow during an incident
- Ensure the integrity of operations and security of your company's assets
- Address future implementation, control enablement, and a road to follow for organizational and prioritization purposes
- Serve as methods of prevention and include what to do in the event a breach does occur, to mitigate any damage and recover as quickly as possible.



The What:

- **Cyber security plan** is a document that outlines how an organization protects its **IT assets** from **cyber threats**.
- It covers the **strategy, policy, procedures, and technologies** that are used to **prevent, detect, and respond to cyber incidents**
- It also defines the **roles and responsibilities** of different **stakeholders**, such as **employees, managers, IT staff, and external partners**.
- A **cyber security plan** should be based on a **risk assessment** that identifies the most likely and **impactful cyber threats** to the organization.
- A **cyber security plan** should be aligned with the **best practices and standards** in the industry, such as the **NIST Cybersecurity Framework**.
- A **cyber security plan** should be **regularly reviewed and updated** to reflect the changing **threat landscape** and the **evolving needs** of the organization



Key Elements:

Five Key Elements of Your Strategic Cybersecurity Plan:

Now it is time to start writing your plan. Here is a proposed layout and details of the critical information to include:

- **Mission statement**
- **Vision statement**
- **Introduction**
- **Governance**
- **Strategic objectives**



The Who:

It's the IT guys... right??



The When:

Start now!



Where to Get Help

Local Groups

Alaska Cyber Group

- Meets via MS Teams the third Thursday of each month
- Open to all SLTT and Critical Infrastructure organizations
- Provide a briefing on current and emerging threats and trends
- Distribution channel on critical cyber threats and events both from CISA and to CISA and to group members
- Forum to share information and ask questions

Cybersecure Alaska (cybersecurealaska.org)

- Non-profit organization promoting a cybersecure business community
- Open to private organizations
- Provide resources for business to assess their cyber security vulnerabilities and develop prevention strategies





For more information:

Contact:
Mark Breunig
Cybersecurity State Coordinator
(907) 795-5673
mark.breunig@cisa.dhs.gov

