

CYBERSECURITY RESILIENCE THROUGH PUBLIC-PRIVATE PARTNERSHIPS

Mark Breunig

Cybersecurity Advisor, Region X (Alaska)

February 15, 2022



Mark Breunig
February 17, 2022

Overview

- CISA Introduction
- Critical Infrastructure
- Make the Case for Partnerships
- CISA Resources and Services



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:



Critical Infrastructure Owners

85% of critical infrastructure is privately-owned

- Federal Emergency Management Agency (FEMA)

“80 percent of America’s businesses have fewer than 10 employees, and 95 percent have fewer than 100.”

- Brian Moynihan, CEO
Bank of America



The Case for Partnerships

Cross-sector threats are the biggest bang for the buck, but difficult for organizations to prevent:

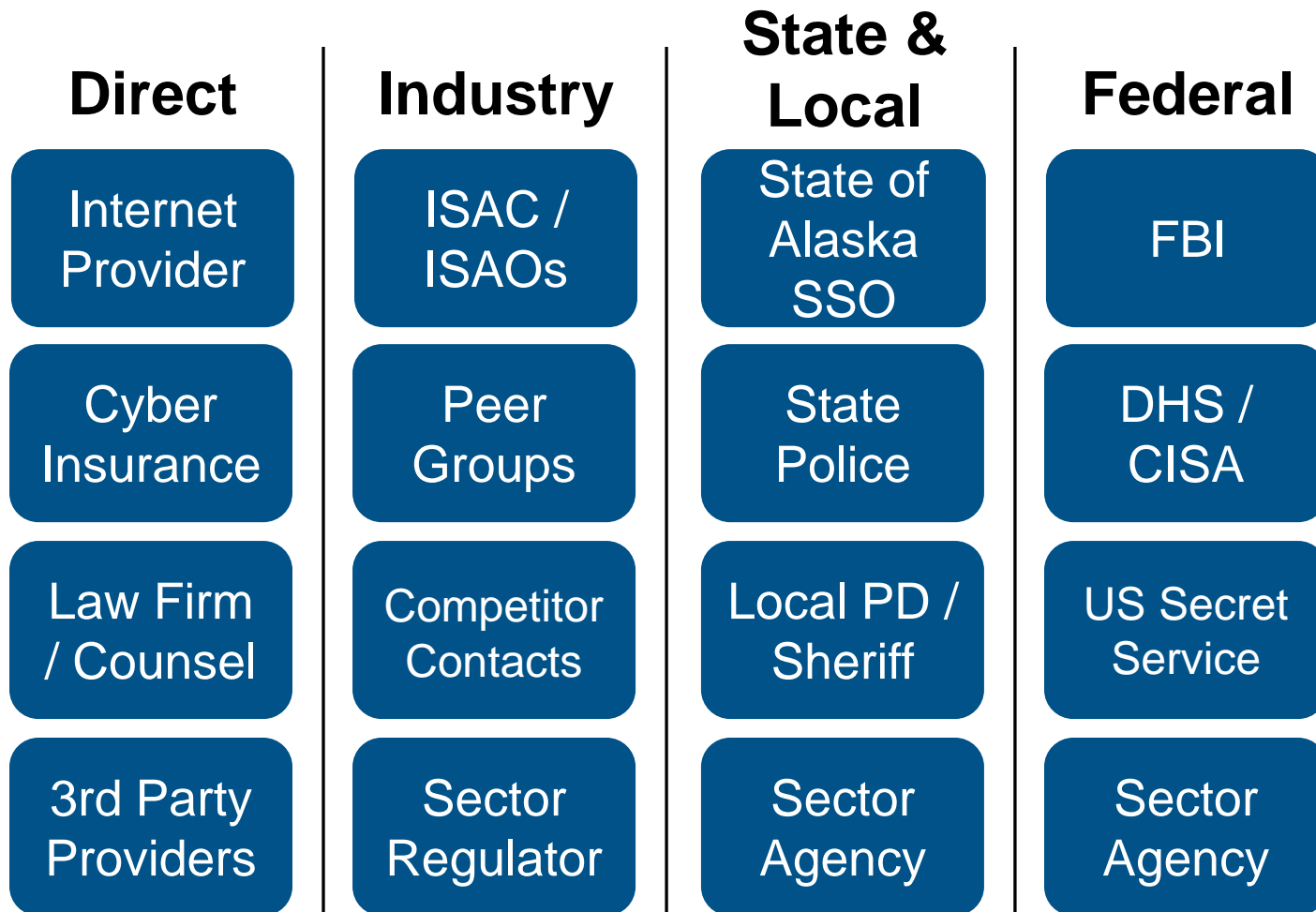
- Ransomware
- Insider threats
- Supply chain attacks
- Phishing



Cybersecurity is a collective problem and requires a collaborative approach



Building a Partner Network



CISA Touchpoints

Cybersecurity Advisors (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



Cybersecurity Offerings

Preparedness Activities

- Information / Threat Indicator Sharing
- Cybersecurity Training and Awareness
- Cyber Exercises and “Playbooks”
- National Cyber Awareness System
- Vulnerability Notes Database
- Information Products and Recommended Practices
- Cybersecurity Evaluations
 - Cyber Resilience Reviews (CRR™)
 - Cyber Infrastructure Surveys
 - Phishing Campaign Assessment
 - Vulnerability Scanning
 - Risk and Vulnerability Assessments (aka “Pen” Tests)
 - External Dependencies Management Reviews
 - Cyber Security Evaluation Tool (CSET™)
 - Validated Architecture Design Review (VADR)

Response Assistance

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

Cybersecurity Advisors

- Assessments
- Working group collaboration
- Best Practices private-public
- Incident assistance coordination

Protective Security Advisors

- Assessments
- Incident liaisons between government and private sector
- Support for National Special Security Events



National Cyber Awareness System

- US-CERT NCAS offers tips and alerts to the public
- Materials and intelligence for various levels of expertise

<https://us-cert.cisa.gov/ncas>



CISA Ransomware Hub

StopRansomware.gov

- One-stop shop for federal ransomware materials
- ***Ransomware Guide***
 - Part 1: Ransomware Prevention Best Practices
 - Part 2: Ransomware Response Checklist



CISA Tabletop Exercise Package

- Self-service or CISA facilitated
- Cyber, Physical, and Cyber-Physical exercises
- Monthly, 90-minute workshops

Download for free:

<https://www.cisa.gov/cisa-tabletop-exercises-packages>



Cybersecurity Assessments



Cybersecurity Assessments



Protected Critical Infrastructure Information

The Protected Critical Infrastructure Information (PCII) program guards your organization's information

Sensitive critical infrastructure information voluntarily given to CISA within the CRR, EDM and CIS assessments is **protected** by law from:

- Public release under Freedom of Information Act (FOIA) requests
- Public release under state, local, tribal, or territorial disclosure laws
- Use in civil litigation
- Use in regulatory purposes



Conclusion

- CISA introduction
- Private sector critical infrastructure
- Partnerships for resilience
- CISA resources and services





For more information:
CISA.gov
StopRansomware.gov

Questions?
Mark.Breunig@cisa.dhs.gov
(907) 795-5673

