INTRODUCTION OF CISA ADVISORS AND SERVICES OFFERED

KS MODERNIZATION COMMITTEE

10 JANUARY 2024

CISA: Defend Today, Secure Tomorrow

As America's Cyber Defense Agency, we lead the national effort to understand, manage, and reduce risk to our critical infrastructure.

John A. Bryant
January 10, 2024

CISA Operational Priorities

CYBER SUPPLY CHAIN AND 5G

CISA is focused on supply chain risk management in the context of national security. CISA is looking to reduce the risks of foreign adversary supply chain compromise in 5G and other technologies.

ELECTION SECURITY

CISA assists state and local governments and the private sector organizations that support them with efforts to enhance the security and resilience of election infrastructure. CISA's objective is to reduce the likelihood of compromises to election infrastructure confidentiality, integrity, and availability, essential to the conduct of free and fair democratic elections.

SOFT TARGET SECURITY

As the DHS lead for the soft targets and crowded places security effort, CISA supports partners to identify, develop, and implement innovative and scalable measures to mitigate risks to these venues; many of which serve an integral role in the country's economy.

FEDERAL CYBERSECURITY

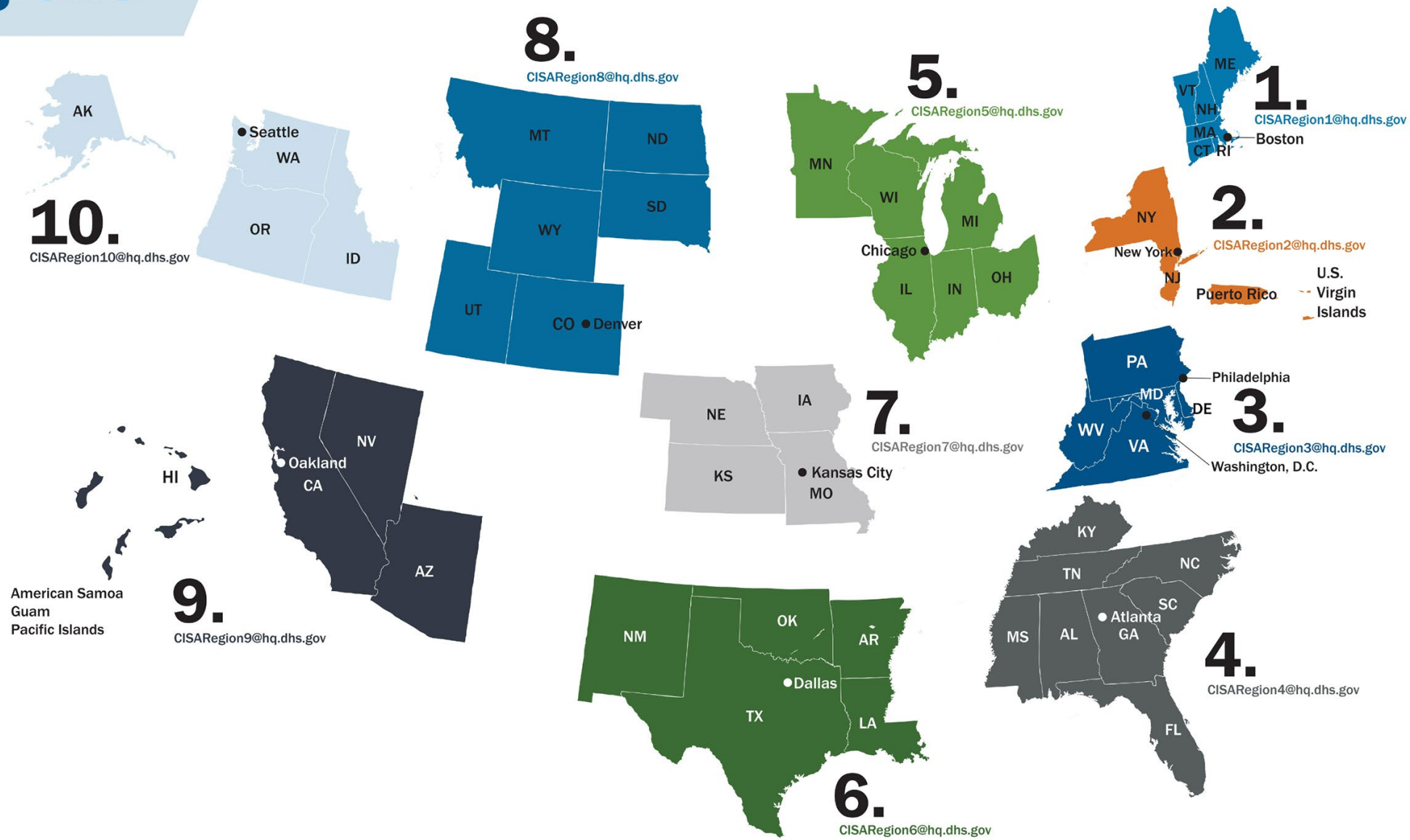
CISA provides technology capabilities, services, and information necessary for agencies across the Federal civilian executive branch to manage sophisticated cybersecurity risks. CISA's authorities enable deployment of robust capabilities to protect Federal civilian unclassified systems, recognizing that continuous improvement is required to combat evolving threats. CISA also works to help State, Local, Tribal and Territorial governments improve cybersecurity and defend against cybersecurity risks.

INDUSTRIAL CONTROL SYSTEMS

CISA leads the Federal Government's unified effort to work with the Industrial control systems (ICS) community to reduce risk to our critical infrastructure by strengthening control systems' security and resilience.

CISA Regions

- 1 Boston, MA
- 2 New York, NY
- 3 Philadelphia, PA
- 4 Atlanta, GA
- 5 Chicago, IL
- 6 Irving, TX
- 7 Kansas City, MO
- 8 Lakewood, CO
- 9 Oakland, CA
- 10 Seattle, WA
- CS Pensacola, FL



Security Advisor Programs

Security Advisors are field-based critical infrastructure security specialists who link State, local, tribal, territorial (SLTT) & private sector stakeholders with infrastructure protection resources

- **Educate:** Inform and raise awareness.
- **Listen:** Collect stakeholder concerns & needs.
- **Promote:** Encourage best practices and risk mitigation strategies.
- **Assess:** Evaluate critical infrastructure risk.
- **Coordinate:** Bring together incident support and lessons learned.
- **Build Capacity:** Initiate, develop capacity, and support communities-of-interest and working groups.

Protective Security Advisors (PSA): Security, Emergency Preparedness, and Business Continuity Programs

Cybersecurity Advisors (CSA): Cybersecurity for Information Technology & Operational Technology networks

Where to Start?: Cyber Hygiene Scanning

Purpose: Assess Internet-accessible systems for known vulnerabilities and configuration errors.

Delivery: Online by CISA

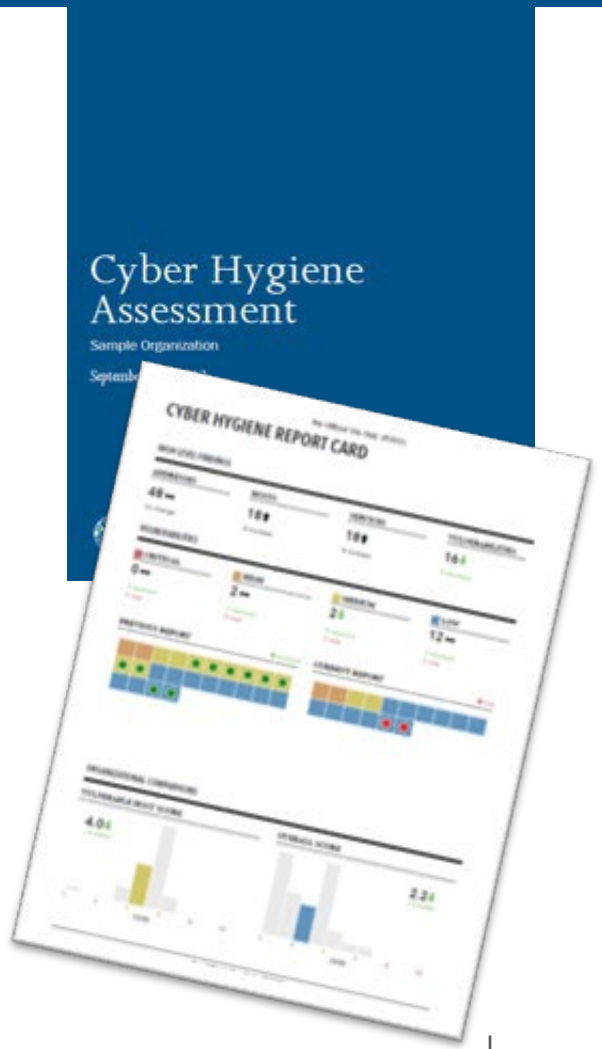
Benefits:

- Continual review of system to identify potential problems
- Weekly reports detailing current and previously mitigated vulnerabilities
- Recommended mitigation for identified vulnerabilities

- **Network Vulnerability & Configuration Scanning**
  - Identify network vulnerabilities and weakness

To get started:

Entity Name:
Address:
POC Name:
POC Email:
POC Phone:



Situational Awareness

National Cyber Awareness System

https://www.cisa.gov/uscert/ncas

Current Activity

Provides up-to-date information about high-impact types of security activity affecting the community at large.

https://www.cisa.gov/uscert/ncas/current-activity

Bulletins

Provide weekly summaries of new vulnerabilities. Patch information is provided when available.

https://www.cisa.gov/uscert/ncas/bulletins

Alerts

Provide timely information about current security issues, vulnerabilities, and exploits.

https://www.cisa.gov/uscert/ncas/alerts

Analysis Reports

Provide in-depth analysis on a new or evolving cyber threat.

https://www.cisa.gov/uscert/ncas/analysis-reports

MULTI-FACTOR AUTHENTICATION

Federal Communications Commission

CISA Urges Organizations to Incorporate the FCC Covered List Into Risk Management Plans | CISA

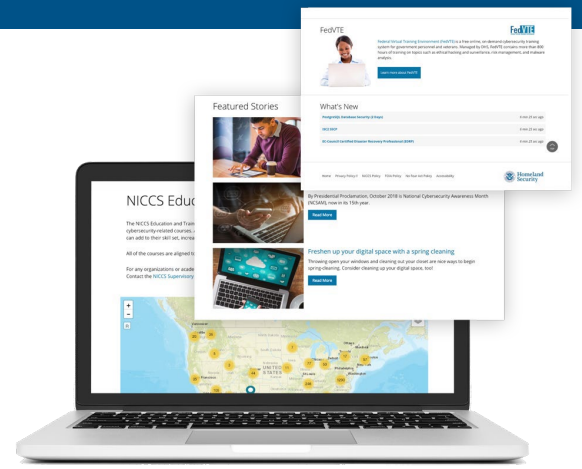
List of Equipment and Services Covered By Section 2 of The Secure Networks Act | Federal Communications Commission (fcc.gov)

CISA.GOV


CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
AMERICA'S CYBER DEFENSE AGENCY
Search
Topics
Spotlight
Resources & Tools
News & Events
Careers
About
REPORT A CYBER ISSUE
SHARE:
CISA: Defend Today, Secure Tomorrow
As America's Cyber Defense Agency, we lead the national effort to understand, manage, and reduce risk to our critical infrastructure.
Click to Report
Click to Subscribe
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA Central
888-282-0870
Central@cisa.dhs.gov

CISA Catalog

CISA is committed to providing the nation with access to cybersecurity training and workforce development efforts to develop a more resilient and capable cyber nation.



- **The NICCS website:** Searchable Training Catalog with over 6,000 cyber- related courses offered by nationwide cybersecurity educators
  - Interactive National Cybersecurity Workforce Framework
    Cyber Career Pathways Tool | NICCS (cisa.gov)
  - **FedVTE - https://fedvte.usalearning.gov**
  - Scholarships for Service, Centers for Academic Excellence, and Cyber Competitions
  - Tools and resources for cyber managers
- Incident Response Training - IMR Series Incident Management Review (IMR) Training | CISA
- Industrial Control Systems (ICS) Training **https://ics-training.inl.gov/learn**
- **TEEX Cyber Readiness Center - https://teex.org/program/cybersecurity/**

For more information, visit https://www.cisa.gov/cybersecurity-training-exercises

Available Service & Tools

- Cyber Security Evaluation Tool (CSET)
- Known Exploited Vulnerabilities (KEV) Catalog
- Bad Practice Catalog
- Get Your Stuff Off Search
- Cyber Essentials Toolkit
- Ransomware Guide
- Free Tools Catalog:
  - Antivirus
  - Malware Removal
  - Investigation
  - Log analysis
  - Scanning
  - Network packet captures
  - Protocol analyzer
  - Intrusion detection & prevention
  - Threat modeling
  - Backup

https://www.cisa.gov/free-cybersecurity-services-and-tools

Additional Information Sharing Opportunities

- **Multi-State Information Sharing and Analysis Center:**
  - Focal point for cyber threat prevention, protection, response and recovery for state, local, tribal, and territorial governments.
  - Operates 24 x7 cyber security operations center, providing real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification and mitigation and incident response. For more information, visit www.cisecurity.org/ms-isac or email info@msisac.org

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Elections Infrastructure ISAC™

- **ISACs and ISAOs:**
  - **Information Sharing and Analysis Centers** (ISACs) or **Organizations** (ISAOs) are communities of interest sharing cybersecurity risk, threat information, and incident management to members. For more information on ISACs, visit www.nationalisacs.org. For more on ISAOs visit www.isao.org/about.

ONG-ISAC

National Defense ISAC

FS-ISAC

RETAIL & HOSPITALITY ISAC

Real Estate ISAC Information Sharing and Analysis Center
Serving the Commercial Facilities Sector

WATER ISAC

SPACE ISAC

CISA Cybersecurity & Infrastructure Security Agency

Maritime Transportation System Information Sharing and Analysis Center

MEISAC MEDIA + ENTERTAINMENT INFORMATION SHARING ANALYSIS CENTER

REN-ISAC

IT ISAC

DNG-ISAC

H-ISAC HEALTH - ISAC

AVIATION ISAC

E-ISAC

AUTO-ISAC Automotive Information Sharing and Analysis Center

TLP: GREEN

MS-ISAC Services

Cybersecurity Services	Description	NO COST	LOW COST
Cyber Threat Intelligence			
Cyber Alerts & Advisories	Brief, timely emails containing information on specific cyber incidents/threats and vulnerabilities in software and hardware	✓	
Quarterly Threat Report	Analysis of SLTT-focused cyber threat intelligence trends and threat forecasting	✓	
Regular IOCs	Weekly, monthly reports on malicious IPs/domains	✓	
White Papers	Technical papers providing relevant information on cyber threat topics	✓	
Cyber Threat Briefings	Informative sessions on the cyber threat landscape to SLTTs	✓	
Real-time Intelligence Feeds	Easy-to-implement real-time cyber threat intelligence indicator feeds derived from more than 200 sources and specific to SLTTs	✓	
Cybersecurity Services			
24x7x365 Security Operations Center (SOC)	Full-time cyber defense partner to member organizations that monitors, analyzes, and responds to cyber incidents affecting members	✓	
Malicious Domain Blocking & Reporting (MDBR)	Web security service that proactively blocks network traffic to known harmful web domains, protecting IT systems against cyber threats	✓	
Endpoint Security Services (ESS)	Device-level protection and response for active defense against both known (signature-based) and unknown (behavioral-based) malicious activity		✓
Albert Network Monitoring and Management	Cost-effective network Intrusion Detection System (IDS) tailored to SLTT governments' threat profile and security needs		✓
Managed Security Services (MSS)	Cost-effective log and security event monitoring of devices like IDS/IPS, firewalls, switches and routers, services, endpoints, and web proxies		✓
Penetration Testing	Services that simulate a real-world cyber attacks on network and web applications and enable organizations to safely identify exploitable vulnerabilities.		✓
Security Best Practices			
CIS SecureSuite Membership	Comprehensive set of cybersecurity resources and tools to implement the CIS Critical Security Controls (CIS Controls) and CIS Benchmarks.	✓	
Other Member Services & Resources			
MS-ISAC Webinars	Monthly member calls and webinars on topics of interest to the SLTT community	✓	
MS-ISAC Working Groups	Voluntary committees focused on collaboration among SLTT organizations to help drive MS-ISAC initiatives and member enrichment and growth	✓	
Nationwide Cybersecurity Review (NCSR)	Anonymous, annual self-assessment designed to evaluate cybersecurity maturity and set a baseline for organizational improvement	✓	
CIS CyberMarket	A collaborative purchasing program available to SLTTs that leverages collective purchasing power of our 14,000+ member organizations to provide low-cost security solutions from industry-leading cybersecurity providers		✓

Example from Texas

Currently, we have this requirement for schools reporting incidents to us, the Texas Education Agency:
https://statutes.capitol.texas.gov/Docs/ED/htm/ED.11.htm#11.175
What this boils down to is if student PII is involved in a malicious attack, then they have to report those events to us.

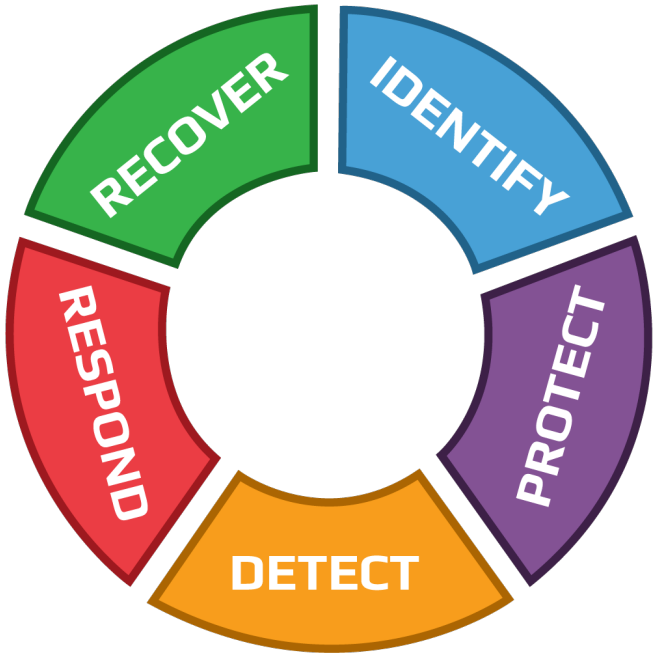
Then generally for data breach of over 250 Texans, there are requirements to report to the Texas Attorney General:
https://statutes.capitol.texas.gov/Docs/BC/htm/BC.521.htm#521.053

There is some proposed legislation that would expand this **current** requirement for state agencies reporting security incidents to be required by **all local governments**:
https://statutes.capitol.texas.gov/Docs/GV/htm/GV.2054.htm#2054.1125

The **proposed** changes are here:
https://capitol.texas.gov/BillLookup/Text.aspx?LegSess=88R&Bill=HB712

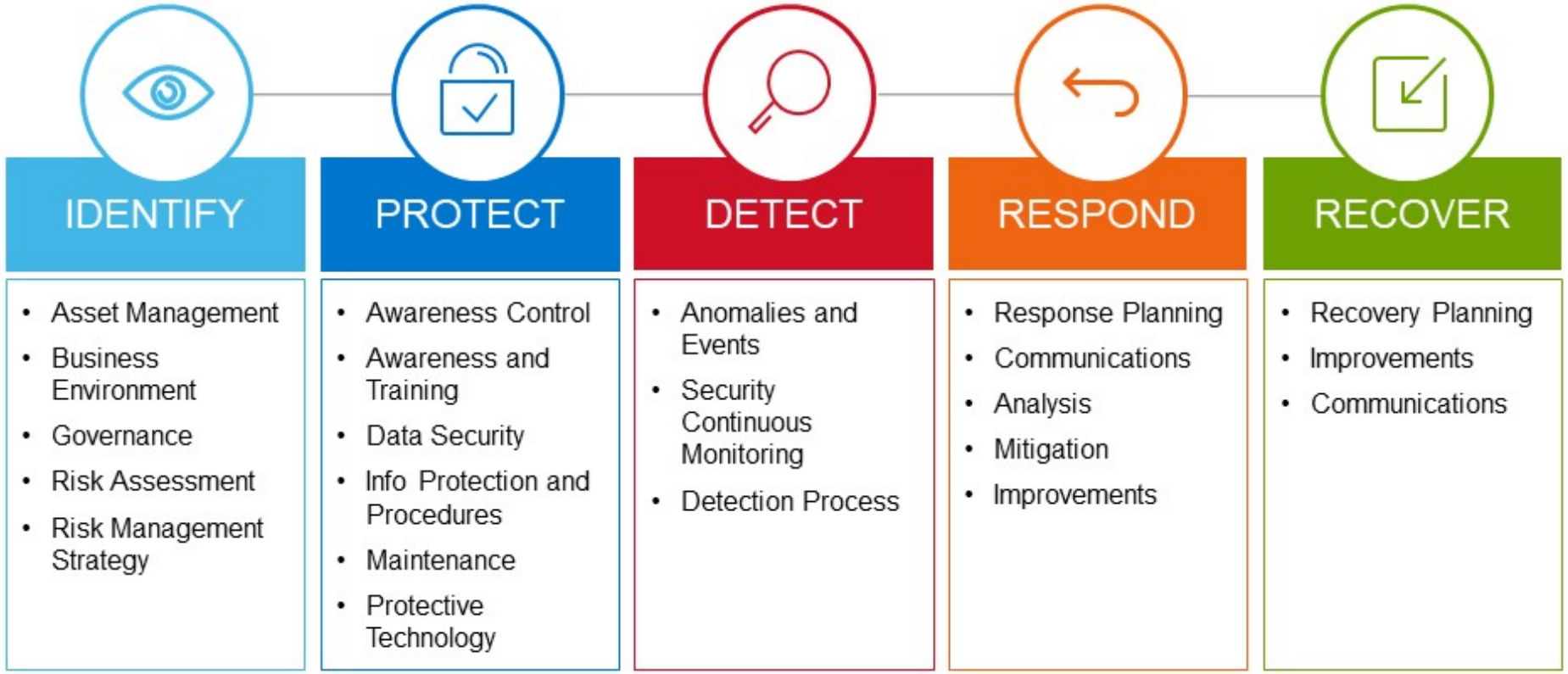
CPG Categories

38 goals align to the NIST Cybersecurity Framework (CSF)



https://www.cisa.gov/cpg

NIST CSF 2.0



Govern

- Mission
- Stakeholder expectations
- Legal requirements
- Risk Management Strategies
- Supply Chain management
- Responsibilities & Authorities
- Policies & Procedures
- Oversight

John A. Bryant
January 10, 2024

Region 7 Security Advisors Kansas

Sam Alva

Cybersecurity Advisor,

316-299-2322

Samuel.alva@cisa.dhs.gov

Chuck Clanahan, CPP

Protective Security Advisor,

North Kansas District

758-213-8699

chuck,.clanahan@cisa.dhs.gov

John Bryant

Cybersecurity Security Advisor

John.bryant@cisa.dhs.gov

Phone: 816-634-0528

Timothy Morgan

Protective Security Advisor,

Southern Kansas District

620-803-7244

timothy.morgan@cisa.dhs.gov

For further information, contact:

CISA.IOD.REGION.R07_Ops@cisa.dhs.gov

Or

Central@cisa.dhs.gov