CYBERSECURITY LANDSCANE AND THREATS TO MARITIME OPERATIONS

Jason Burt
Cybersecurity Advisor, Region IV
Cybersecurity Advisor Program
Cybersecurity and Infrastructure Security Agency

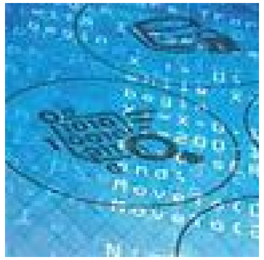
Divisions of CISA

- CISA consists of:

Cybersecurity Division

Infrastructure Security Division

Emergency Communications Division



National Risk Management Center

CISA Mission and Vision

Cybersecurity and Infrastructure Security Agency (CISA)

Mission:

- Lead the collaborative national effort to strengthen the security and resilience of America’s critical infrastructure

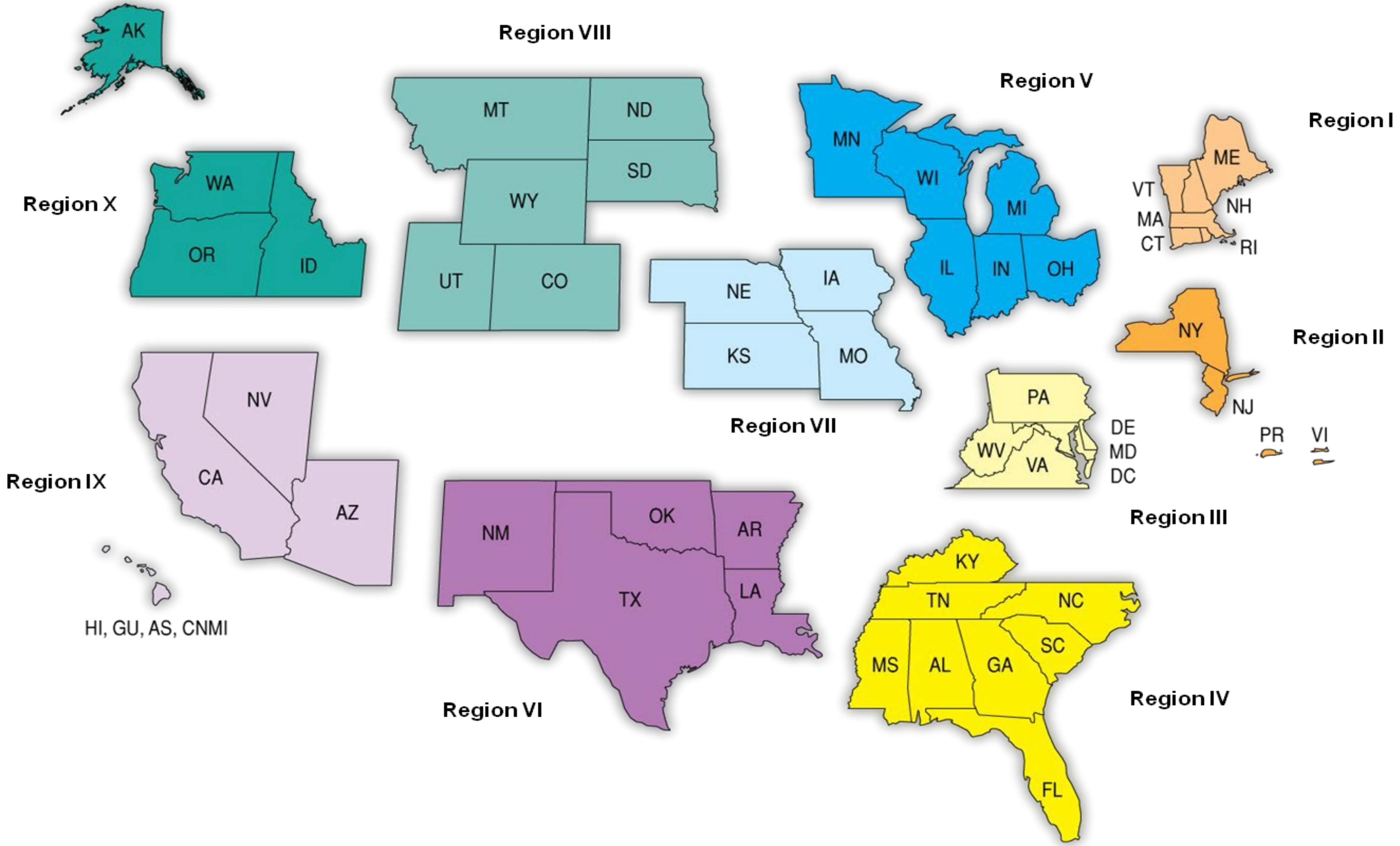
Vision:

- A Nation with secure, resilient, and reliable critical infrastructure upon which the American way of life can thrive

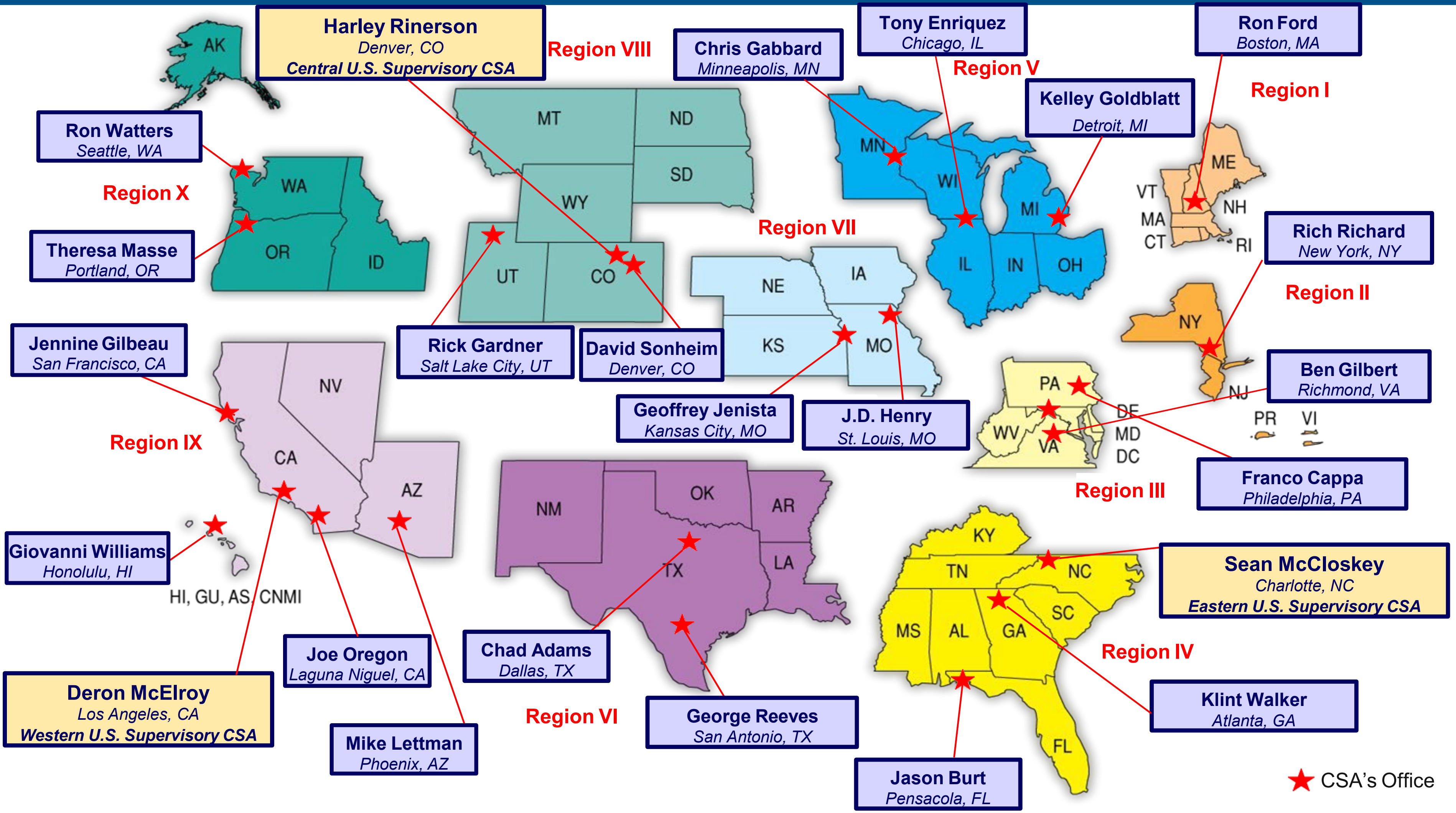
CYBERSECURITY ADVISOR PROGRAM

Jason Burt
August 10, 2021

CSA Regionally Deployed Personnel



CSA Regionally Deployed Personnel



Harley Rinerson
Denver, CO
Central U.S. Supervisory CSA

Region VIII

Chris Gabbard
Minneapolis, MN

Tony Enriquez
Chicago, IL

Region V

Ron Ford
Boston, MA

Kelley Goldblatt
Detroit, MI

Region I

Ron Watters
Seattle, WA

Region X

Theresa Masse
Portland, OR

Region VII

Rich Richard
New York, NY

Region II

Jennine Gilbeau
San Francisco, CA

Rick Gardner
Salt Lake City, UT

David Sonheim
Denver, CO

Ben Gilbert
Richmond, VA

Geoffrey Jenista
Kansas City, MO

J.D. Henry
St. Louis, MO

Region IX

Franco Cappa
Philadelphia, PA

Region III

Giovanni Williams
Honolulu, HI

HI, GU, AS, CNMI

Sean McCloskey
Charlotte, NC
Eastern U.S. Supervisory CSA

Chad Adams
Dallas, TX

Joe Oregon
Laguna Niguel, CA

Region IV

Deron McElroy
Los Angeles, CA
Western U.S. Supervisory CSA

Region VI

Klint Walker
Atlanta, GA

Mike Lettman
Phoenix, AZ

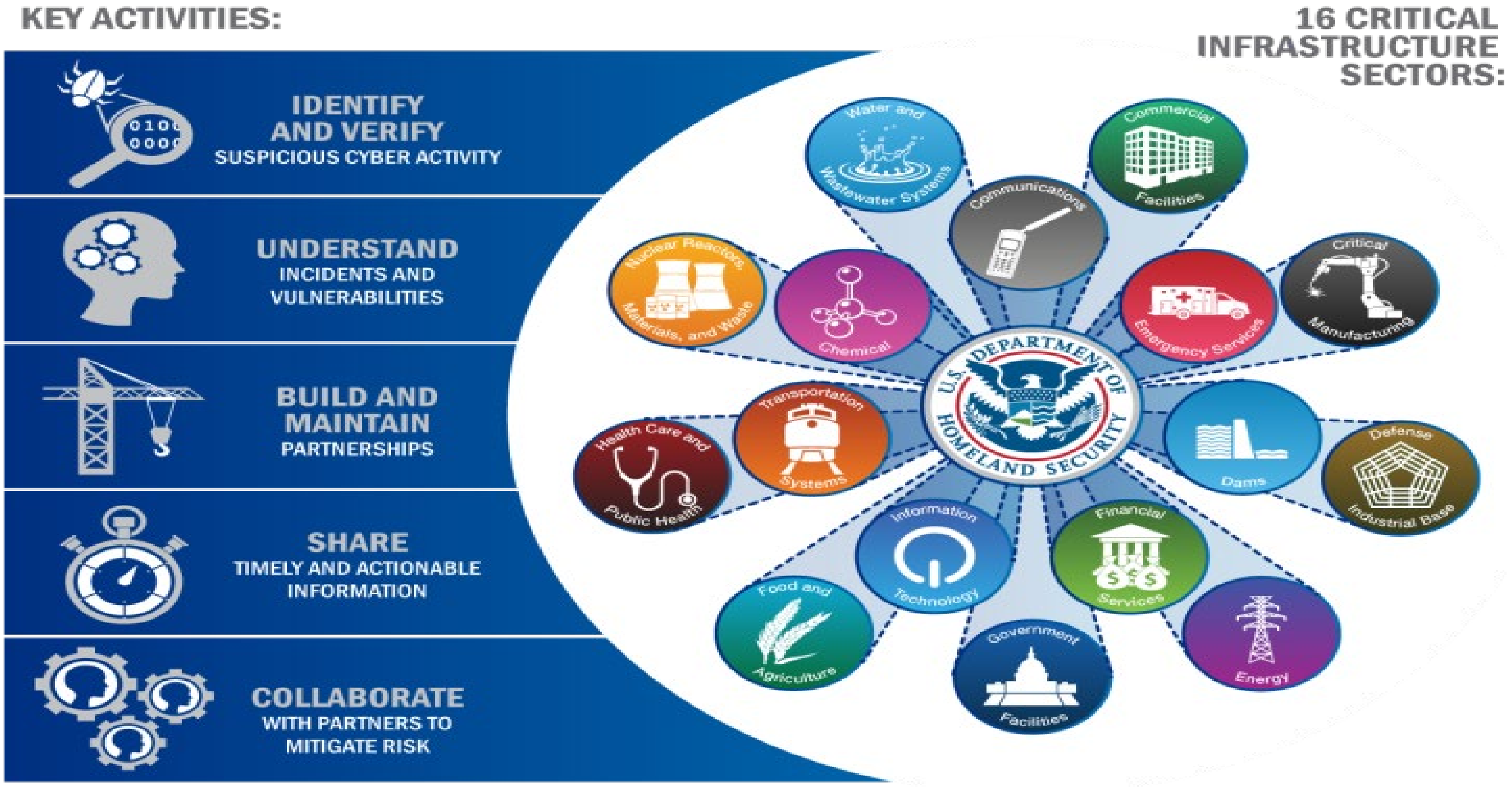
George Reeves
San Antonio, TX

Jason Burt
Pensacola, FL

★ CSA's Office

Jason Burt
August 10, 2021

Serving Critical Infrastructure



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:

CYBER THREATS

Today's Risk Landscape

America remains at risk from a variety of threats:

- ACTS OF TERRORISM
- CYBER ATTACKS
- EXTREME WEATHER
- PANDEMICS
- ACCIDENTS OR TECHNICAL FAILURES

PORT FACILITY CYBERSECURITY RISKS

Port Components at Risk

1 Facility Access

The degradation or disruption of systems used to identify and direct cargo, truck drivers, and facility personnel can cause significant congestion or the closure of the terminal until systems restoration is complete.

2 Terminal Headquarters – Data

Malicious actors may access information systems within the terminal in order to access sensitive client and cargo information. Malicious actors may also attempt to use this information to steal cargo or smuggle illicit cargo through the terminal.

3 Terminal Headquarters – Ransomware

The manipulation or destruction of data, most commonly seen in ransomware attacks, can disrupt operations within a facility until systems and data can be restored from reliable, isolated backups. Previous attacks have resulted in facilities being partially or completely offline for days, resulting in significant business losses.

4 Operational Technology (OT) Systems

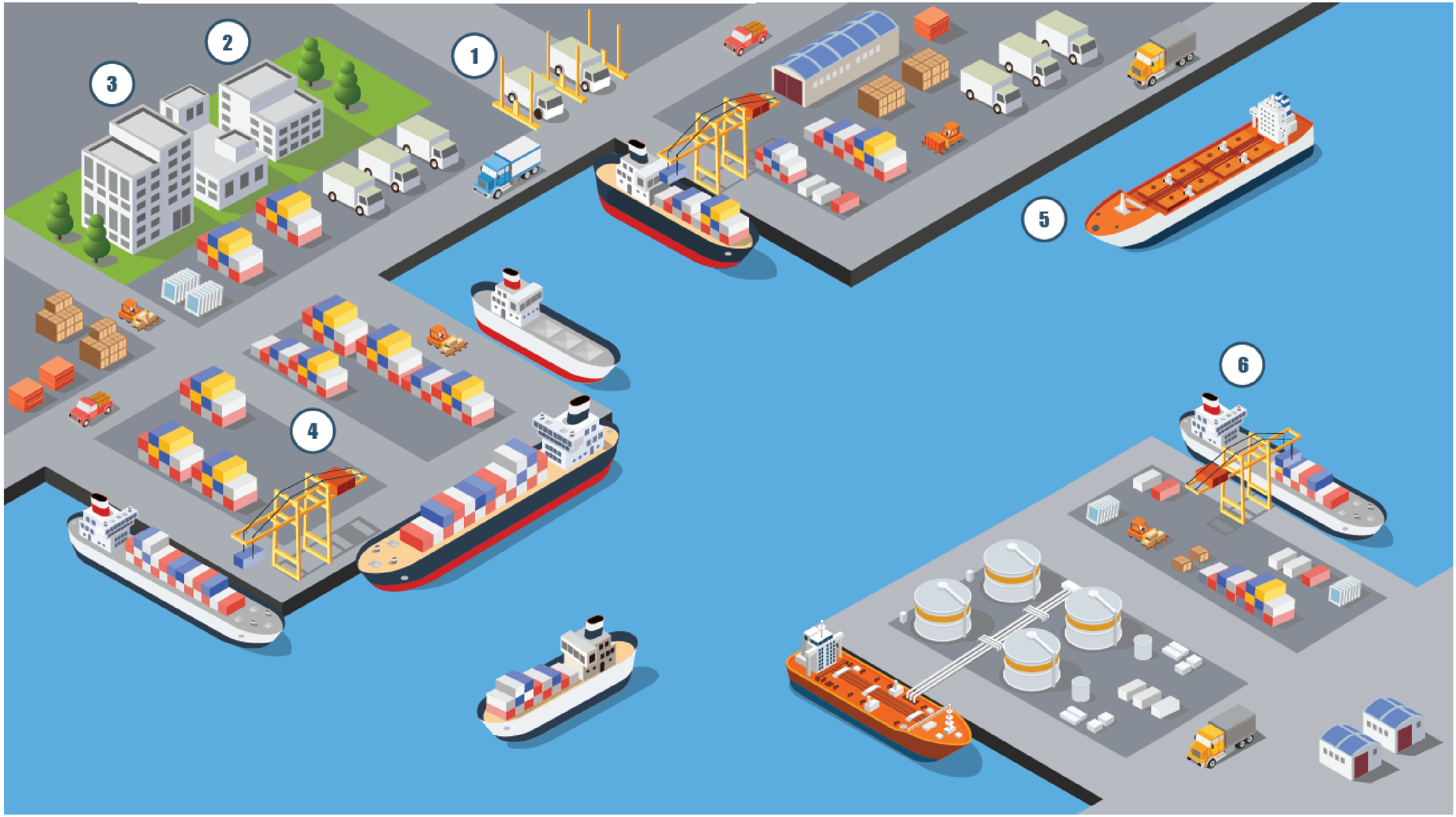
OT Systems – systems, devices, and communications links used to control physical processes at ports, including cargo handling equipment and pumps – are being increasingly incorporated into maritime facilities. The compromise of OT systems could cause changes to cargo movements, interrupt port operations, and cause physical damage to equipment and safety risks for personnel.

5 Positioning, Navigation, and Timing (PNT)

Position, Navigation, and Timing is pervasive throughout the Maritime subsector, and plays an essential role in many maritime functions such as vessel navigation and port logistics. Loss of PNT services would disrupt vessel movements in the port and complex logistics systems at port facilities. Loss of PNT could also lead to collisions and allisions, resulting in potential damage to fixed infrastructure, pollution, release of hazardous material, fires, loss of life, vessel sinking, and blocking of a navigable channel.

6 Vessel

Compromised systems aboard a vessel or inside a port facility could lead to the compromise of additional waterside or landside systems. Interconnectivity between berthed vessels and maritime facilities through the sharing of Wi-Fi, network connections, USB storage devices, etc. can lead to system compromises that otherwise may not have occurred.



Jason Burt
August 10, 2021

MARITIME CYBER INCIDENTS

29 Sept 2020 – **Ransomware Attack** – Four largest Maritime Shipping companies attacked since 2017

- 2020 – French shipping co CMA CGM – **Ransomware**; Mediterranean Shipping Company – **Malware**;
- 2018 – COSCO – **Ransomware**; 2017 – APMMaersk – **NotPetya Ransomware/wiper**

30 Dec 2020 – **Maritime Industry on high alert** – Managing Director, Global Maritime Consultants Group (CMCG)

- “The maritime industry will remain a target of cyber-criminals in 2021 and the world’s shipping fleets will need to be on high alert for cyber-attacks as the industry recovers from the damage caused by the global pandemic.”
- “The recent cyber-attacks on companies such as Google demonstrate the sophistication and capabilities of many of the cyber-criminals who have set their sights on the maritime sector.”

2 Jun 2021 – **Ransomware Attack** – Massachusetts Steamship Authority

- Travel delays experienced due to attack on Steamship Authority’s website.
- Website offline for > 7 days; affecting routes to Martha’s Vineyard and Nantucket

Carnival Cruise Lines – Attacked 3 times; Norwegian Cruise Line hit by Ransomware – Dec 2020

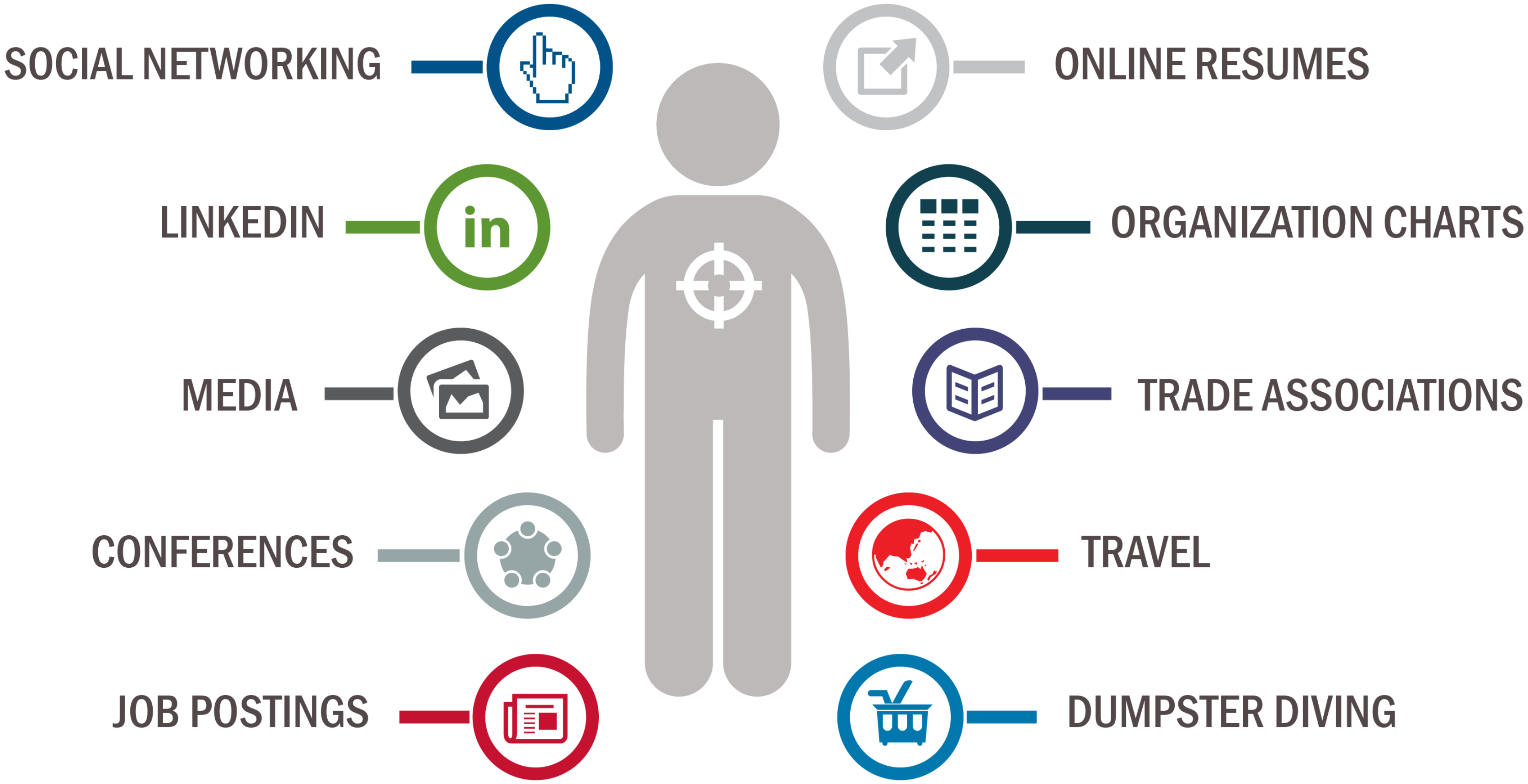
Sources:
https://www.securityweek.com/ransomware-attack-hits-nantucket-marthas-vineyard-ferry-service

https://www.dailymail.co.uk/news/article-9646583/China-hacked-MTA-failed-control-NY-subway-Ransomware-cripples-Marthas-Vineyard-ferry.html

https://seanews.co.uk/security/cyber-security/cybersecurity-will-remain-a-maritime-threat-in-2021/

https://www.zdnet.com/article/all-four-of-the-worlds-largest-shipping-companies-have-now-been-hit-by-cyber-attacks/

HOW ARE YOU TARGETED?



SOCIAL NETWORKING

LINKEDIN

MEDIA

CONFERENCES

JOB POSTINGS

ONLINE RESUMES

ORGANIZATION CHARTS

TRADE ASSOCIATIONS

TRAVEL

DUMPSTER DIVING

Social Engineering Red Flags

FROM

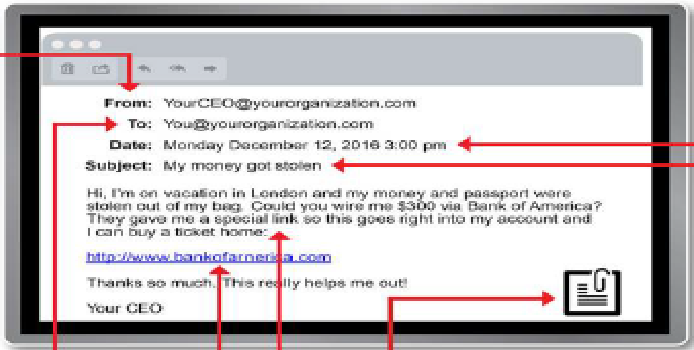
- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."



From: YourCEO@yourorganization.com
To: You@yourorganization.com
Date: Monday December 12, 2016 3:00 pm
Subject: My money got stolen

Hi, I'm on vacation in London and my money and passport were stolen out of my bag. Could you wire me $300 via Bank of America? They gave me a special link so this goes right into my account and I can buy a ticket home:

http://www.bankofarnerica.com

Thanks so much. This really helps me out!

Your CEO

DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

Especially under the prevailing conditions – Always Pause and Ask:

Is this message expected?

Do I recognize the sender of this email?

Is there something odd about the email address?

Verify the email address/domain by hovering the cursor over an email address or embedded link, without clicking; the actual destination appears in a text box or bubble.

Is there a needlessly urgent call to action in the email?

Is the action sought odd or unfamiliar?

Are my network access credentials requested after clicking to open a link?

NEVER enter user name and password in these circumstances!

Be Attentive – and Protect Yourself and the Network

PHISHING EXAMPLE #1

To: <Stakeholder List>

From: Apples Customer Relations <freeapplesforyou@apple.org>

Subject: Free iPad – Just Complete a Survey!

Want the new iPad or iPad Mini? I got mine free from this site: https://apple.com/giveaway !!!!!

We would like to invite you to be part of a brand new pilot program to get our new product in the hands of users before official release. This assures that any issues or errors are mitigated before the release. If you are accept to participate in this programall we ask is that you submit a survey at the end of the Pilot. You be able to keep iPad at the end for free!

Apples Customer Relationships Office

Apples Campus, Cupertino, California 95114

PHISHING EXAMPLE #2

To: <Stakeholder List>
From: OBRM <OBRM@organization.org>
Subject: Future Budget Plans

In the coming weeks, our state’s leadership will be working to draft a plan to prevent long term financial issues and ways to avoid human resource reductions. All departments within the State Government are being directed to draft a plan to help meet projected budget shortages and find ways to reduce spending within the State Government.

We have been asked to work more efficiently with less. As a result, many budgets and programs are also facing significant reduction. The Office of Budget and Resource Management has developed a draft plan that will address any potential budget shortcomings.

To learn more about the budget and how your program maybe affected, please visit https://www.organization.org/budget

If you have any questions or concerns, we’d love to hear them. Please emails us here budget@organization.org

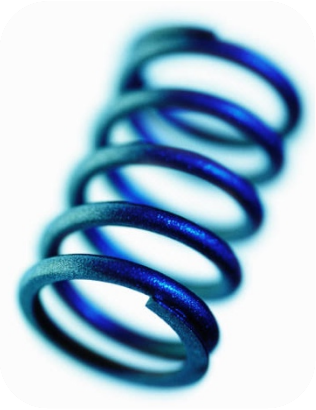
Office of Budget and Resource Management

OPERATIONAL RISK & CYBER RESILIENCY

Resilience Defined

"… the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents…"

- Presidential Policy Directive 21
February 12, 2013



Protect (Security)	**Sustain (Continuity)**
Perform (Capability)	**Repeat (Maturity)**

Emergent Property of Operational Resilience

- The **emergent property** of infrastructure requires an entity to
  - Prevent disruptions from occurring and
  - Respond quickly and recover from disruptions in its most critical business processes.
- Emergent property of operational resilience is essential to critical infrastructure.

What Is An Emergent Property?

- Consider your health.
  - How do you become healthy?
  - Can you buy good health?
  - Can you “manufacture” good health?
- *Good health* and *resilience* are both emergent properties.
- They develop – or emerge – from what we do.

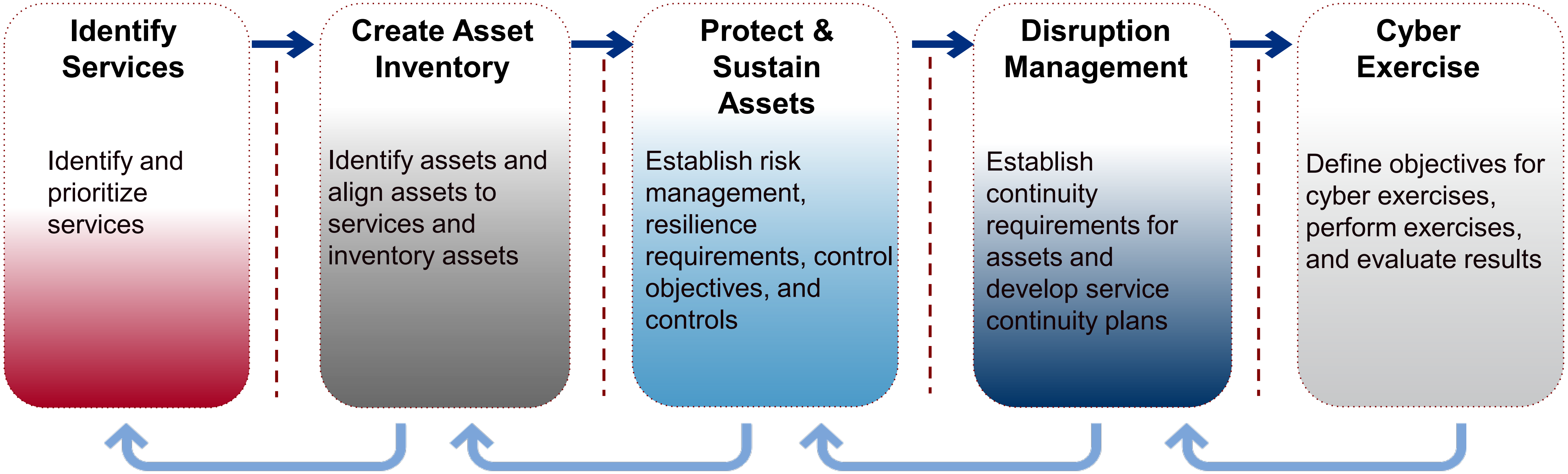
Operational Resilience in Practice

Operational resilience emerges from what we do, such as:

- Identifying and mitigating risks,
- Planning for and managing vulnerabilities and incidents,
- Performing service-continuity processes and planning,
- Managing IT operations,
- Managing, training, & deploying people,
- Protecting and securing important assets, and
- Working with external partners.

Working toward Cyber Resilience

Follow a framework or general approach to cyber resilience.
One successful approach includes:



Identify Services

Identify and prioritize services

Create Asset Inventory

Identify assets and align assets to services and inventory assets

Protect & Sustain Assets

Establish risk management, resilience requirements, control objectives, and controls

Disruption Management

Establish continuity requirements for assets and develop service continuity plans

Cyber Exercise

Define objectives for cyber exercises, perform exercises, and evaluate results

Process Management and Improvement

CISA CYBER SERVICES

Criticality of Periodic Assessments

- Periodic assessments are essential for resilience
- Can’t protect if you don’t know what needs protection
- Can’t fix what needs if you don’t know what’s wrong

Protected Critical Infrastructure Information Program

Protected Critical Infrastructure Information (PCII) Program Guards Your Information

- Sensitive critical infrastructure information voluntarily given to CISA is protected by law from
  - Public release under Freedom of Information Act requests,
  - Public release under State, local, tribal, or territorial disclosure laws,
  - Use in civil litigation and
  - Use in regulatory purposes.

Jason Burt
August 10, 2021

Range of Cybersecurity Services

STRATEGIC
(C-Suite Level)

- Cyber Resilience Review (Strategic)
- External Dependencies Management (Strategic)
- Cyber Infrastructure Survey (Strategic)
- Cybersecurity Evaluations Tool Strategic/Technical)
- Phishing Campaign Assessment (EVERYONE)
- **Vulnerability Scanning / Hygiene (Technical)**
- Validated Architecture Design Review (Technical)
- Risk and Vulnerability Assessment (Technical)

TECHNICAL
(Network-Administrator Level)

VULNERABILITY SCANNING / HYGIENE

Vulnerability Scanning / Hygiene

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

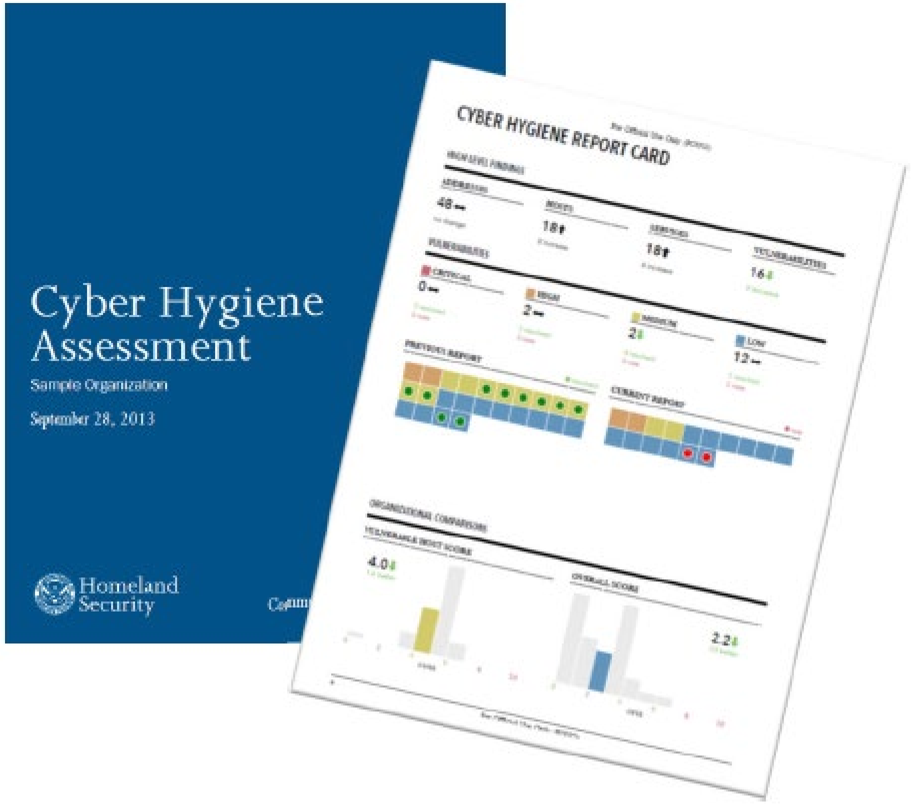
Delivery: Identify public-facing Internet security risks, through service enumeration and vulnerability scanning online by CISA.

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



Cyber Hygiene Assessment

Sample Organization

September 28, 2013

Homeland Security

CYBER HYGIENE REPORT CARD

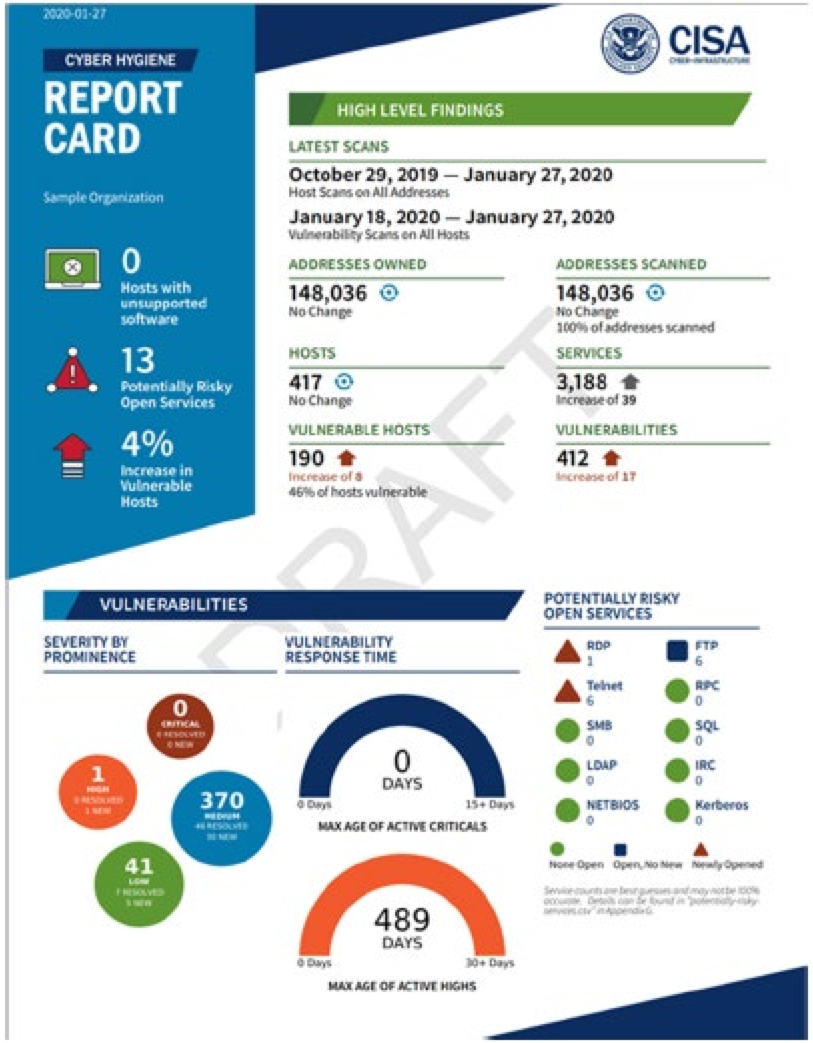
Cyber Hygiene Report Card

High Level Findings

- Latest Scans
- Addresses Owned
- Addresses Scanned
- Hosts
- Services
- Vulnerable Hosts
- Vulnerabilities

Vulnerabilities

- Severity by Prominence
- Vulnerability Response Time
- Potentially Risky Open Services



2020-01-27

CYBER HYGIENE

REPORT CARD

Sample Organization

0 Hosts with unsupported software

13 Potentially Risky Open Services

4% Increase in Vulnerable Hosts

CISA CYBER+INFRASTRUCTURE

HIGH LEVEL FINDINGS

LATEST SCANS

October 29, 2019 — January 27, 2020
Host Scans on All Addresses

January 18, 2020 — January 27, 2020
Vulnerability Scans on All Hosts

ADDRESSES OWNED
148,036
No Change

ADDRESSES SCANNED
148,036
No Change
100% of addresses scanned

HOSTS
417
No Change

SERVICES
3,188
Increase of 39

VULNERABLE HOSTS
190
Increase of 8
46% of hosts vulnerable

VULNERABILITIES
412
Increase of 17

VULNERABILITIES

SEVERITY BY PROMINENCE

0 CRITICAL 0 RESOLVED 0 NEW

1 HIGH 0 RESOLVED 1 NEW

370 MEDIUM 46 RESOLVED 30 NEW

41 LOW 7 RESOLVED 5 NEW

VULNERABILITY RESPONSE TIME

0 DAYS
0 Days 15+ Days
MAX AGE OF ACTIVE CRITICALS

489 DAYS
0 Days 30+ Days
MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

▲ RDP 1	■ FTP 6
▲ Telnet 6	● RPC 0
● SMB 0	● SQL 0
● LDAP 0	● IRC 0
● NETBIOS 0	● Kerberos 0

● None Open ■ Open, No New ▲ Newly Opened

Service counts are best guesses and may not be 100% accurate. Details can be found in "potentially-risky-services.csv" in Appendix G.

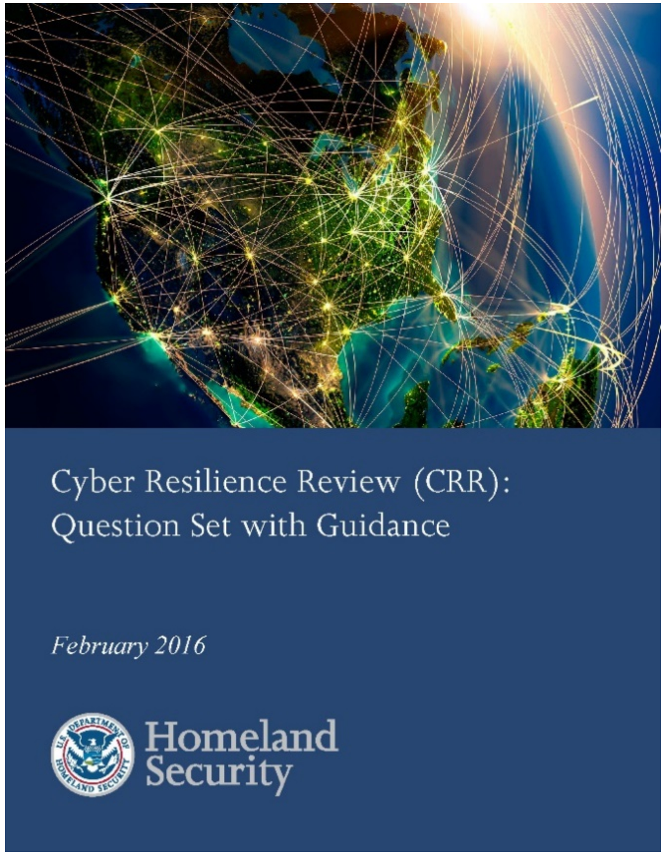
CYBER RESILIENCE REVIEW

Cyber Resilience Review

- **Purpose:** Evaluate operational resilience and cybersecurity practices of **critical services.**

- Delivery: Either
  - CSA-facilitated, or
  - Self-administered

- Benefits include: Helps public and private sector partners understand and measure cybersecurity capabilities as they relate to operational resilience and cyber risk



Cyber Resilience Review (CRR): Question Set with Guidance

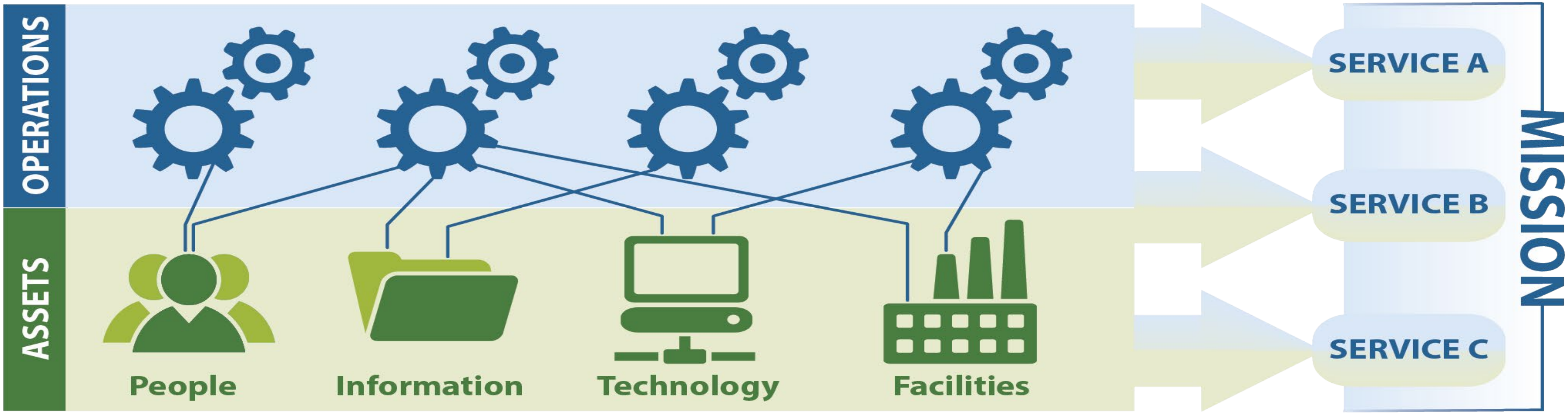
February 2016

Homeland Security

CRR Question Set & Guidance

Critical Service Focus

Organizations use **assets (people, information, technology, and facilities)** to provide operational **services** and accomplish **missions.**



Jason Burt
August 10, 2021

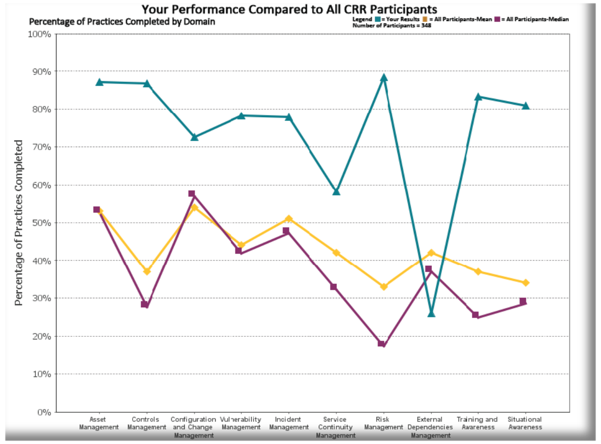
Cyber Resilience Review Domains

Asset Management Know your assets being protected & their requirements, e.g., CIA	**Risk Management** Know and address your biggest risks that considers cost and your risk tolerances
Configuration and Change Management Manage asset configurations and changes	**Service Continuity Management** Ensure workable plans are in place to manage disruptions
Controls Management Manage and monitor controls to ensure they are meeting your objectives	**Situational Awareness** Discover and analyze information related to immediate operational stability and security
External Dependencies Management Know your most important external entities and manage the risks posed to essential services	**Training and Awareness** Ensure your people are trained on and aware of cybersecurity risks and practices
Incident Management Be able to detect and respond to incidents	**Vulnerability Management** Know your vulnerabilities and manage those that pose the most risk

For more information: http://www.us-cert.gov/ccubedvp

CRR Sample Report

Each CRR report includes:

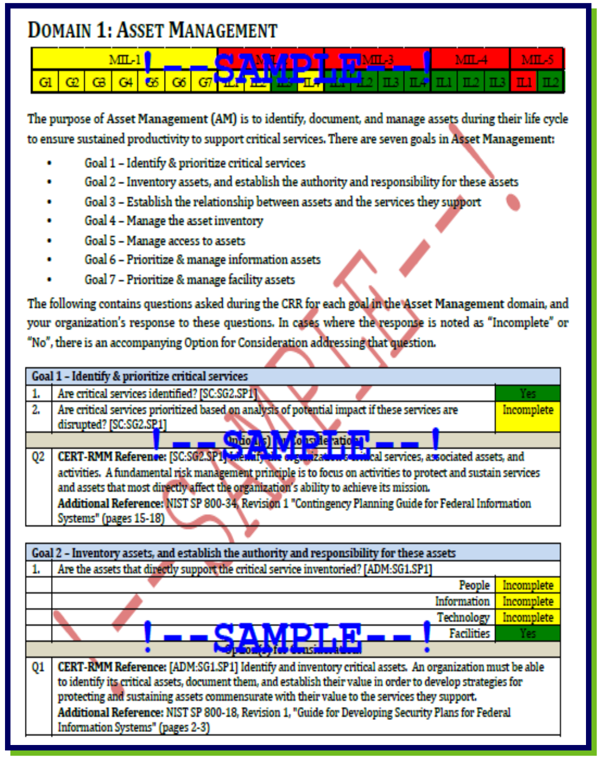


Comparison data with other CRR participants
**facilitated only*

NIST Cybersecurity Framework Summary
NIST CSF Summary
Legend
FUNCTION
CATEGORY
Identify (ID)
Protect (PR)
Detect (DE)
Respond (RS)
Recover (RC)
BUSINESS CONFIDENTIAL

A summary “snapshot” graphic, related to the **NIST Cyber Security Framework**.

Domain performance of existing cybersecurity capability and options for consideration for all responses



Domain 1: Asset Management

MIL-1							MIL-2				MIL-3				MIL-4			MIL-5	
G1	G2	G3	G4	G5	G6	G7	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL1	IL2

The purpose of Asset Management (AM) is to identify, document, and manage assets during their life cycle to ensure sustained productivity to support critical services. There are seven goals in Asset Management:

- Goal 1 – Identify & prioritize critical services
- Goal 2 – Inventory assets, and establish the authority and responsibility for these assets
- Goal 3 – Establish the relationship between assets and the services they support
- Goal 4 – Manage the asset inventory
- Goal 5 – Manage access to assets
- Goal 6 – Prioritize & manage information assets
- Goal 7 – Prioritize & manage facility assets

The following contains questions asked during the CRR for each goal in the Asset Management domain, and your organization's response to these questions. In cases where the response is noted as “Incomplete” or “No”, there is an accompanying Option for Consideration addressing that question.

Goal 1 – Identify & prioritize critical services		
1.	Are critical services identified? [SC:SG2.SP1]	Yes
2.	Are critical services prioritized based on analysis of potential impact if these services are disrupted? [SC:SG2.SP1]	Incomplete
Option(s) for Consideration		
Q2	**CERT-RMM Reference:** [SC:SG2.SP1] Identify the organization's critical services, associated assets, and activities. A fundamental risk management principle is to focus on activities to protect and sustain services and assets that most directly affect the organization's ability to achieve its mission. **Additional Reference:** NIST SP 800-34, Revision 1 "Contingency Planning Guide for Federal Information Systems" (pages 15-18)	

Goal 2 – Inventory assets, and establish the authority and responsibility for these assets		
1.	Are the assets that directly support the critical service inventoried? [ADM:SG1.SP1]	
	People	Incomplete
	Information	Incomplete
	Technology	Incomplete
	Facilities	Yes
Option(s) for Consideration		
Q1	**CERT-RMM Reference:** [ADM:SG1.SP1] Identify and inventory critical assets. An organization must be able to identify its critical assets, document them, and establish their value in order to develop strategies for protecting and sustaining assets commensurate with their value to the services they support. **Additional Reference:** NIST SP 800-18, Revision 1, "Guide for Developing Security Plans for Federal Information Systems" (pages 2-3)	

EXTERNAL DEPENDENCIES MANAGEMENT ASSESSMENT

Jason Burt
August 10, 2021

EDM Assessment Organization and Structure

- Structure and scoring similar to Cyber Resilience Review
- Uses one Maturity Indicator Level (MIL) scale with three lifecycle domains.

Relationship Formation

Assesses whether the acquirer evaluates and controls the risks of relying on external entities before entering into relationships with them.

Relationship Management and Governance

Assesses whether the acquirer manages ongoing relationships to maintain the resilience of the critical service, and mitigate dependency risk.

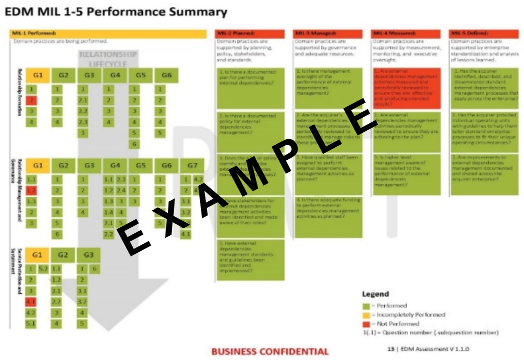
Service Protection and Sustainment

Assesses whether the acquirer accounts for its dependence on external entities as part of its operational activities around managing incidents, disruptions, and threats.

EDM Assessment Report

Each EDM report includes:

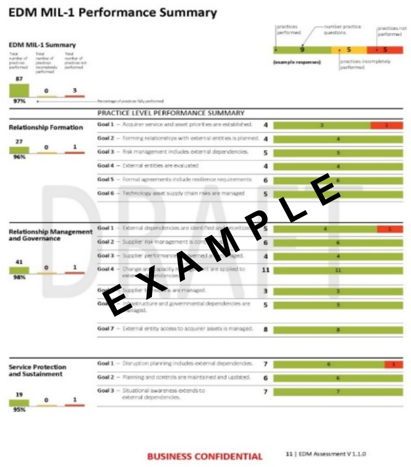
- Performance summary of existing capability managing external dependencies


EDM MIL 1-5 Performance Summary

EXAMPLE

BUSINESS CONFIDENTIAL

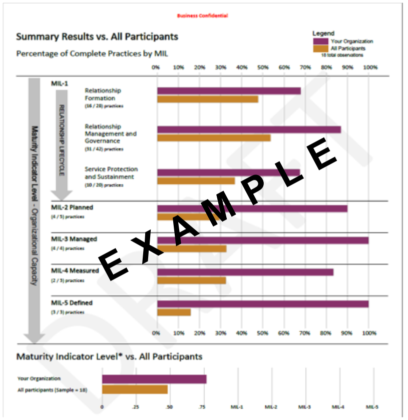
- Comparison data with other EDM participants


EDM MIL-1 Performance Summary

PRACTICE LEVEL PERFORMANCE SUMMARY

EXAMPLE

BUSINESS CONFIDENTIAL

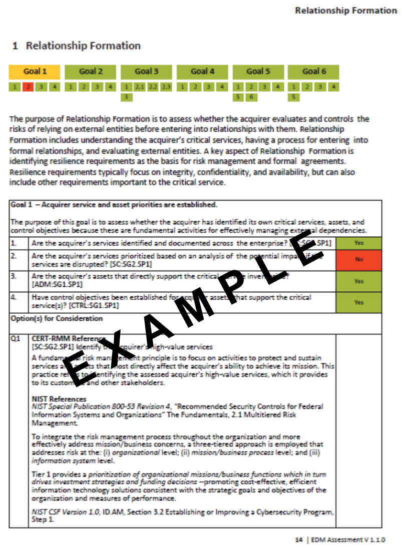

Summary Results vs. All Participants

Percentage of Complete Practices by MIL

Maturity Indicator Level* vs. All Participants

EXAMPLE

- Sub-domain performance of existing capability managing external dependencies and options for consideration for all responses


Relationship Formation

1 Relationship Formation

EXAMPLE

Jason Burt
August 10, 2021

CYBER INFRASTRUCTURE SURVEY

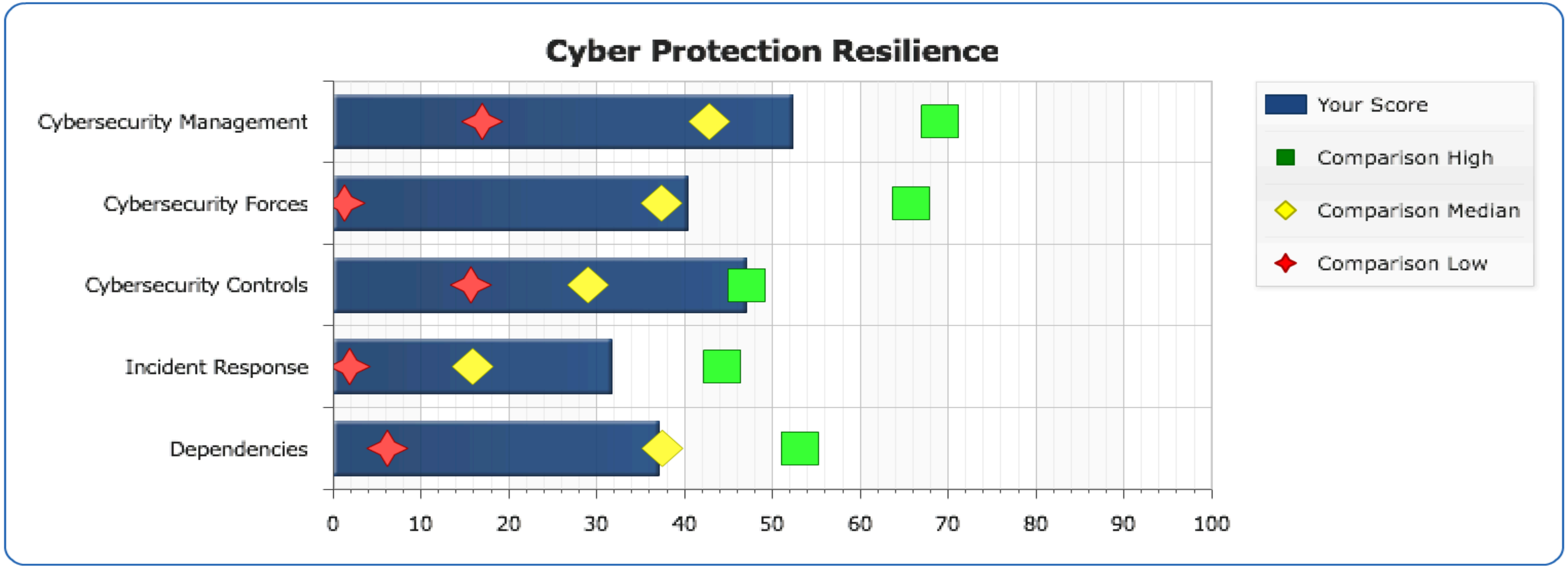
Jason Burt
August 10, 2021

Cyber Infrastructure Survey (CIS)

- Purpose: Evaluate security controls, cyber preparedness, overall resilience.
- Delivery: CSA-facilitated
- Benefits:
  - Effective assessment of cybersecurity controls in place for a critical service,
  - Easy-to-use interactive dashboard to support cybersecurity planning and resource allocation.

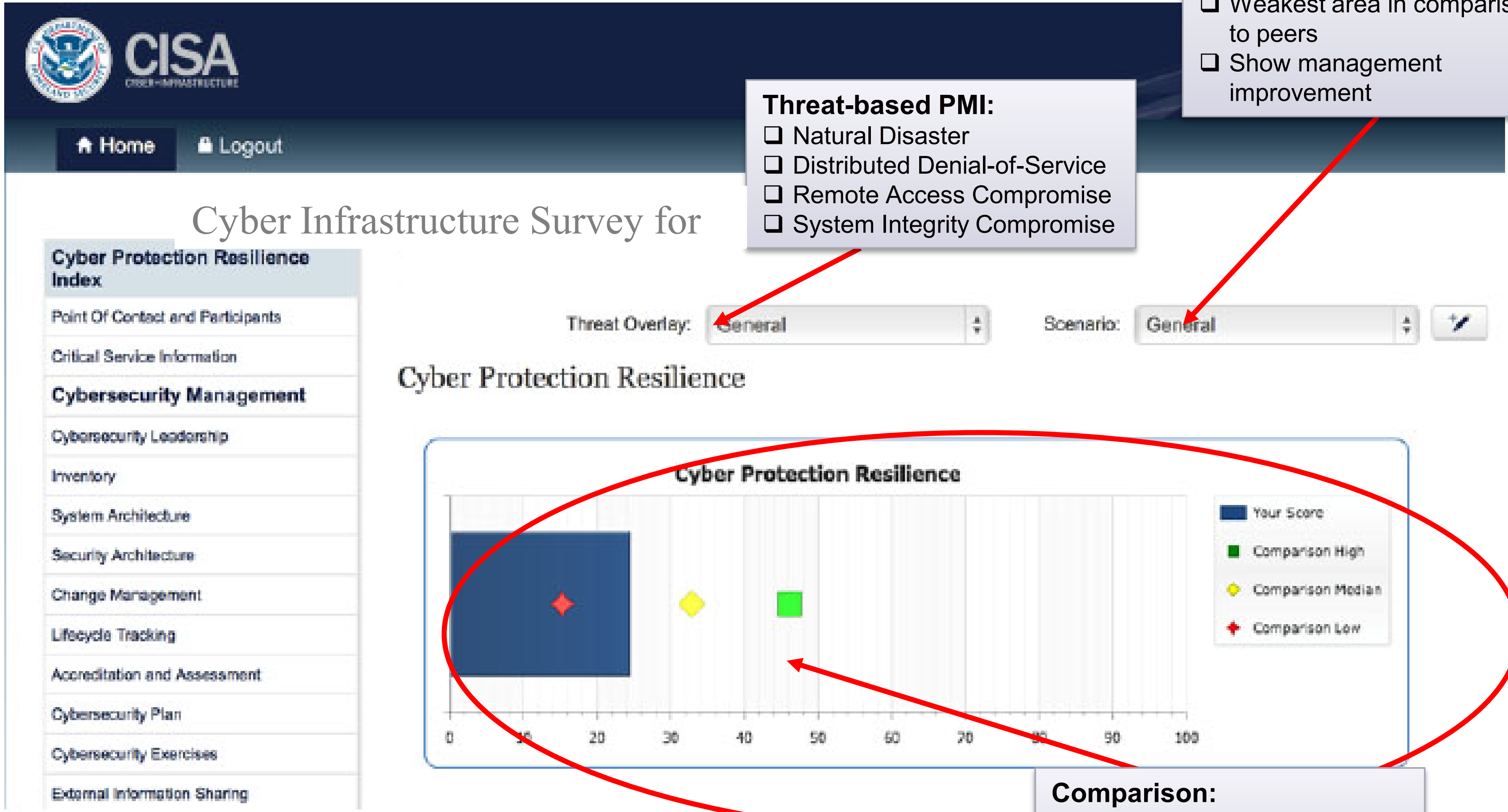
CIS Dashboard - Comparison

- Shows the low, median, and high performers
- Compares your organization to the aggregate



Jason Burt
August 10, 2021

Example of CIS Dashboard



Cyber Infrastructure Survey for

- Cyber Protection Resilience Index
- Point Of Contact and Participants
- Critical Service Information
- **Cybersecurity Management**
- Cybersecurity Leadership
- Inventory
- System Architecture
- Security Architecture
- Change Management
- Lifecycle Tracking
- Accreditation and Assessment
- Cybersecurity Plan
- Cybersecurity Exercises
- External Information Sharing

Threat Overlay: General

Scenario: General

Cyber Protection Resilience

Threat-based PMI:

- ❑ Natural Disaster
- ❑ Distributed Denial-of-Service
- ❑ Remote Access Compromise
- ❑ System Integrity Compromise

Scenario:

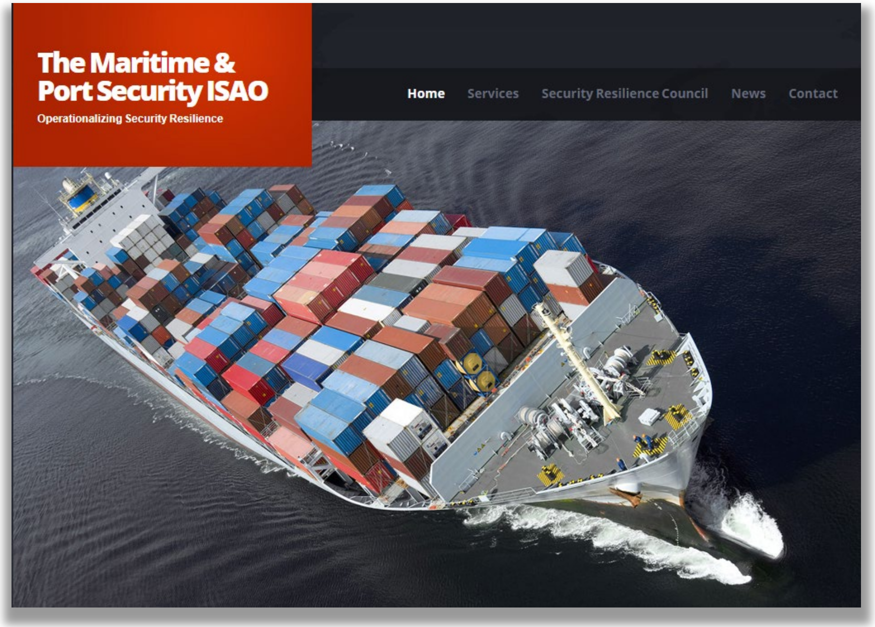
- ❑ Where should we to invest?
- ❑ Weakest area in comparison to peers
- ❑ Show management improvement

Comparison:

- ❑ Low Performers
- ❑ Median Performers
- ❑ High Performers

MARITIME CYBERSECURITY RESOURCES

- Port and Maritime Cyber Resilience
  www.mpsisao.org
- CISA National Cyber Awareness System
  https://us-cert.cisa.gov/ncas
- CISA - Stop Ransomware Campaign
  https://www.cisa.gov/stopransomware
- CISA – Port Facility Cyber Risks
  https://www.cisa.gov/publication/port-facility-cybersecurity-risks


The Maritime & Port Security ISAO
Operationalizing Security Resilience
Home
Services
Security Resilience Council
News
Contact

Contact

CISA Contact Information	
Jason Burt Region IV Cybersecurity Advisor (Alabama, Mississippi, Florida)	Jason.Burt@cisa.dhs.gov (202) 578-9954 (Cell)
Klint Walker Region IV Cybersecurity Advisor (Georgia, Tennessee, Kentucky)	Klint.Walker@hq.dhs.gov (404) 895-1127 (Cell)
Sean McCloskey Region IV Cybersecurity Advisor (North Carolina, South Carolina)	Sean.McCloskey@hq.dhs.gov (202) 578-8853 (Cell)