PORT CYBERSECURITY WORKSHOP

OVERVIEW

2024 Port Cybersecurity Workshop

PURPOSE

The purpose of the Port Cybersecurity Workshop is to provide a focused cyber threat update for our region's seaports and inland ports; present case studies of recent cyber intrusions/attacks at U.S. ports; discuss current port and maritime facilities' cyber readiness; and review government assets and resources available to assist.

It is anticipated that this will the first of several (ongoing) workshops, exercises, activities to enhance cybersecurity in Gulf ports.

2024 Port Cybersecurity Workshop

CONCEPT

- 2-3 Day Workshop
- Port Executives and Cybersecurity/Security personnel

Day 1 - THREAT

- Attuned to Port Executives
- Keynote Speaker
- Threat Assessment, Case Studies of Cyberattacks on Ports

Day 2 - RESOURCES

- Available Resources (Government)

Day 3 – WORK TASKS

- Breakout Sessions to develop Workshop Products

2024 Port Cybersecurity Workshop

WORKSHOP OBJECTIVES

Days 1-2

- Assess threats posed by cyberattacks to port operations and security
- Examine instances (case studies) of Cybersecurity attacks/ intrusions on our Nation's ports
- Identify/assess port cybersecurity gaps and issues
- Identify available government cyber resources
- Discuss best practices to enhance port and maritime cybersecurity

2024 Port Cybersecurity Workshop

WORKSHOP TASKS/OBJECTIVES

1) Create an Appendix for Port Security Plans of contacts to Federal, State, and Regional cybersecurity assets and intelligence agencies;
2) Create a Port protocol for response to a cyber intrusion and/or attack;
3) Identify recommended actions to be performed per MARSEC levels;
4) Develop a road map of recommended actions to improve ports capabilities and readiness to defend against cyber attacks;
5) Develop template position (job) announcements with recommended hiring prerequisites and preferences for port cybersecurity personnel;
6) Develop draft legislation for the creation of Port Cyber Resilience Center(s) in Texas as used in Europe and at Port Los Angeles;
7) Create a template for a port cybersecurity report modeled after Texas' BOSA

2024 Port Cybersecurity Workshop

PARTICIPATING AGENCIES

- U.S. Coast Guard
- CISA
- FBI
- U.S. Customs and Border Protection
- Borders, Trade, and Immigration Institute
- State Of Louisiana Department Of Transportation And Development
- Texas Department Of Information Resources
- Texas Department Of Transportation (Maritime)
- Ports Association Of Louisiana
- Texas Ports Association
- State and Regional Intelligence Fusion Centers
- InfraGard

PORT CYBERSECURITY WORKSHOP

THE THREAT

December 10, 2024

2024 Port Cybersecurity Workshop

AGENDA

DAY 1, TUESDAY, DECEMBER 10TH

0800 – Registration

0850 – Administrative Announcements: Keiton C. Moore, USCG

0900 – Welcome: CAPTAIN Keith Donohue, Commander, USCG
Sector Houston-Galveston

0915 – Introductions

2024 Port Cybersecurity Workshop

AGENDA

DAY 1, TUESDAY, DECEMBER 10TH

0930 – Workshop Overview:

Kevin Clement, Executive Director SP, BTI Institute

1000 – Break

1030 – Keynote Address:

RDML Jason Tama, Commander, USCG Cyber Command

1100 - CISA

Deron McElroy, Regional Chief of Cybersecurity, CISA

2024 Port Cybersecurity Workshop

WELCOME: COMMANDER, USCG SECTOR

Captain Keith M. Donohue is the Commander, Sector Houston-Galveston in June of 2023. In this position he serves as Captain of the Port, Officer-in-Charge of Marine Inspection, Federal Maritime Security Coordinator, and Federal On-Scene Coordinator.

Captain Donohue oversees all maritime safety, security, environmental protection, search and rescue, emergency response, waterways management, regulatory compliance, and contingency planning for all U.S. navigable waterways from the east bank of the Colorado River in Southwest Texas to 60 miles east of Lake Charles, Louisiana, and 200 miles offshore.

2024 Port Cybersecurity Workshop

WORKSHOP OVERVIEW

Synopsis: Explain the purpose and provide a 20-minute overview of the three-day proceedings, brief workshop objectives, explain the event focus by day, introduce presentations, identify workshop tasks (request sign-up), explain use of “fill in the blank” Appendix: Cyber Contacts.

Kevin Clement is the Executive Director, Strategic Partnerships of the Borders, Trade, and Immigration Institute, *a DHS Center of Excellence led by the University of Houston*. He is the founder and Director of the annual Port of the Future Conference and Director of the Center of Research Excellence to Counter Human Trafficking (CRECHT).

KEYNOTE SPEAKER

2024 Port Cybersecurity Workshop

KEYNOTE SPEAKER

RADM JASON TAMA

Rear Admiral Jason Tama is a prominent figure in the U.S. Coast Guard, currently serving as the Commander of the U.S. Coast Guard Cyber Command. He has a distinguished career spanning over two decades, with significant roles including Senior Director of the National Security Council at The White House.

In his current role, RADM Tama focuses on enhancing cybersecurity initiatives to protect maritime critical infrastructure and ensure the security of Coast Guard operations across various domains.

2024 Port Cybersecurity Workshop

KEYNOTE SPEAKER

DERON MCELROY

Deron McElroy is Chief of Cybersecurity for the Cybersecurity and Infrastructure Security Agency (CISA), Region 6. He leads a team of Cybersecurity Advisors focused on enhancing our Nation's cyber resilience.

As co-founder of the Cybersecurity Advisor Program, he served as Chief of Operations and was the first DHS Cybersecurity Advisor for the Western United States. Previously, he led the interagency development of the Nation's cyber incident response policy and contributed to cybersecurity education and workforce development efforts. Deron played a primary role in the stand-up of the National Cybersecurity and Communications Integration Center and was a key participant in information sharing policy development.

LUNCH BREAK

2024 Port Cybersecurity Workshop

AGENDA

DAY 1, TUESDAY, DECEMBER 10TH

1330 – Case Study: Port Houston Cyberattack
Chris Wolski, CEO, Applied Security Convergence (ASC)

1430 – Port Cyber Insurance
Edward McNamara, CEO, Applied Security Convergence

1530 – Break

1600 – Best Practices to Reduce Port Cyber Vulnerabilities
Lieutenant Daria Read, U.S. Coast Guard Cyber Command

1730 – End Day 1

2024 Port Cybersecurity Workshop

CASE STUDY: PORT HOUSTON

Speaker: **Chris Wolski**, former CISO, Port Houston

Synopsis: In August 2021, Port Houston was the target of a cyberattack reportedly involving ManageEngine ADSelfService Plus, a password management program. The port issued a statement, stating it had successfully defended against an attempted hack in August and "no operational data or systems were impacted."

Cybersecurity and Infrastructure Security Agency Director Jen Easterly initially disclosed that the port was the target of an attack at a Senate committee hearing. She said she believed a "nation-state actor" was behind the hack.

2024 Port Cybersecurity Workshop

PORT CYBER INSURANCE

Insurance can play a key role in helping ports pay for recovery costs if subject to a cyber-attack. It can also cover third-party liabilities.

When looking at port cyber insurance, evaluating your port's overall cybersecurity capabilities across all areas and the exposure to risk is a good starting point for port and terminal operators.

Ports are advised to present the strongest picture to would-be insurers in order to secure the best coverage and reduce premiums. Insurers look for hard evidence of robust risk management policies and protocols, including well-prepared cybersecurity policies, along with regular assessments and continuous employee training.

Ports should include identifying potential threats, assessing the value and sensitivity of the data handled, and evaluating current security measures.

Speaker: **Edward McNamara** , CEO, Armada Risk Partners

2024 Port Cybersecurity Workshop

BEST PRACTICES - REDUCE VULNERABILITIES

Lieutenant Daria Read,
US Coast Guard Cyber Command

Synopsis: A great number of current cyber vulnerabilities experienced by ports can be remediated through acknowledged best practices.

This presentation focuses on best practices in cybersecurity that ports can readily enact to improve their security posture.

BTI Institute
Borders • Trade • Immigration
A Department of Homeland Security Center of Excellence

PORT CYBERSECURITY WORKSHOP

CYBER RESOURCES

December 11, 2024

2024 Port Cybersecurity Workshop

AGENDA

DAY 2, WEDNESDAY, DECEMBER 11TH

0800 – Case Study: Port of Los Angeles Cyber Resilience Center

0900 – U.S. Customs and Border Protection Cyber Response (Cargo and Associates)

Bradford Slutsky, Cargo Security and Controls Division, USCBP

1000 – Break

1030 - U.S. Coast Guard Cyber Resources

Lieutenant Daria Read, USCG Cyber Command

1115 - CISA Cyber Resources

George Reeves, Cybersecurity Advisor, CISA

2024 Port Cybersecurity Workshop

AGENDA

DAY 2, WEDNESDAY, DECEMBER 11TH

1330 – FBI Cyber Resources
SSA Nowell Agent, Federal Bureau of Investigation

1400 – Fusion Center Maritime Analysts
Bill Myers, Senior Police Officer, Houston Police Department
Marisa Brusuelas, Maritime Intelligence Analyst, State of Texas

1430 - Break

1500 – State of Louisiana: Cyber Emergency Response
Corey Bourgeois, State of Louisiana, GOSHEP

1600 - InfraGard: A Force Multiplier
Marco Ayala, President, Houston-Galveston InfraGard

2024 Port Cybersecurity Workshop

PORT CYBER RESILIENCE CENTERS

Increased use of digital technologies, while resulting in greater efficiencies and cargo planning capabilities, subject ports to cybersecurity risks and threats of disruptions to port operations and the supply chain as a whole.

IBM operates the Port of Los Angeles Cyber Resilience Center, an automated port community cyber defense solution, designed by Port of Los Angeles supply chain stakeholders. The CRC serves as an early warning detector against possible cyberattacks and an information resource to help minimize intrusions and restore operations following an attack.

Darious Moore, Delivery Program Executive,
IBM Consulting Cybersecurity Services

2024 Port Cybersecurity Workshop

USCBP CYBER RESPONSE

Synopsis: CBP is a key stakeholder in the area of cyber security in the Port of Entry Environment. CBP regularly engages on potential or actual cyber security incidents in relation to cargo control. There are many platforms and applications that interact with CBP, specifically the Automated Commercial Environment (ACE).

In the eco system at the Ports of Entry, disruption to trade data flow or accessibility to trade information through a breach in systems can cause a risk to interconnectivity to CBP systems. It is imperative that best practices are followed to prevent cyber security incidents, and when encountered that there is a robust response to mitigate the situation.

Speaker: **Bradford Slutsky,**
Cargo Security and Controls Division,
Office of Field Operations, USCBP

2024 Port Cybersecurity Workshop

CISA CYBER RESOURCES

Synopsis: Cybersecurity Advisor George Reeves will provide an introduction to CISA's Cybersecurity Advisory Program and the available no-cost cyber resources available to assist our Maritime/Port Security partners with their cybersecurity efforts.

Speaker: **George Reeves**, Cybersecurity Advisor, CISA

2024 Port Cybersecurity Workshop

USCG CYBER RESOURCES

Synopsis: An overview of the U.S. Coast Guard's enhanced role in port and maritime cybersecurity and those resources available to ports and maritime assets.

Speaker: **TBD**, USCG

Panelist: **TBD**, USCG

LUNCH BREAK

2024 Port Cybersecurity Workshop

FBI CYBER RESOURCES

Synopsis: The FBI is the lead federal agency for investigating cyber attacks and intrusions. The FBI collects and share intelligence and engage with victims while working to unmask those committing malicious cyber activities, wherever they are.

The FBI works with its federal counterparts, foreign partners, and the private sector to close those gaps. These partnerships enhance the FBI's ability to defend networks, attribute malicious activity, sanction bad behavior, and take the fight to our adversaries. The FBI fosters this team approach through unique hubs where government, industry, and academia form long-term trusted relationships to combine efforts against cyber threats.

Speaker: **Special Agent Nowell Agent**
Federal Bureau of Investigation

2024 Port Cybersecurity Workshop

STATE AND REGIONAL FUSION CENTERS

Synopsis: This presentation will provide an overview of the Texas Fusion Center (TxFC) and the Houston Regional Intelligence Service Center (HRISC) and demonstrate how these two fusion centers support the maritime domain. In addition, the presenters will provide a short brief on the origin and scope of their respective programs and outline program priorities. Lastly, the presenters will highlight any areas where they are contributing to overall maritime domain awareness, including anything that could impact the security, safety, economy, or environment.

Speaker: **Maria Bruselas**, Maritime Intelligence Analyst, Texas DPS

Speaker: **Bill Meyers**, Senior Police Officer, Houston Police Department
Houston Regional Intelligence Service Center

2024 Port Cybersecurity Workshop

STATE OF LOUISIANA CYBER RESPONSE

Synopsis: Corey Bourgeois joined The Governor's Office of Homeland Security and Emergency Preparedness and the ESF-2 team in January 2022 as the Cyber Incident Response Director of Louisiana.

Prior to joining the team, he was appointed as the Internet Crimes Against Children (ICAC) Commander of Louisiana. He is also credited for developing the state's first digital forensic laboratory. His extensive background in digital forensics allows him to educate and advise legislators to strengthen laws to protect Louisiana from online child sexual abuse. He holds a degree from Louisiana State University.

Speaker: **Corey Bourgeois**, Cyber Incident Response Director, GOSHEP, Louisiana

2024 Port Cybersecurity Workshop

INFRAGARD RESOURCES

InfraGard is a partnership between the Federal Bureau of Investigation (FBI) and members of the private sector for the protection of U.S. Critical Infrastructure. Through seamless collaboration, InfraGard connects owners and operators within critical infrastructure to the FBI, to provide education, information sharing, networking, and workshops on emerging technologies and threats. InfraGard's membership includes business executives, entrepreneurs, lawyers, security personnel, military and government officials, IT professionals, academia and state and local law enforcement—all dedicated to contributing industry-specific insight and advancing national security.

Speaker: **Marco Ayala**, President, Houston-Galveston InfraGard Chapter

Panelist: **Chris Wolski**, Houston-Galveston InfraGard Chapter

PORT CYBERSECURITY WORKSHOP

BREAK OUT SESSIONS

September 12, 2024

2024 Port Cybersecurity Workshop

AGENDA

DAY 3, THURSDAY, DECEMBER 12TH

0830 – Overview and Assignment of Teams

0900 – Break Out Sessions (Iteration 1)

- **Create an Appendix for Port Security Plans of contacts to Federal, State, and Regional cybersecurity assets and intelligence agencies;**
- **Identify recommended cybersecurity actions to be performed at various MARSEC levels; (Sean Plankey, Chris Wolski)**
- **Create a Port protocol for response to a cyber intrusion and/or attack; (CSA George Reeves, Jennifer Marusak, CSA Todd Vasilou)**
- **Draft legislation for the creation of Port Cyber Resilience Center(s) as used in Europe and at Port Los Angeles (Kevin Clement)**

1130 – Brief Backs

LUNCH BREAK

2024 Port Cybersecurity Workshop

AGENDA

DAY 3, THURSDAY, DECEMBER 12TH

1200 – Lunch Break

1330 – Break Out Sessions (Iteration II)

- **Develop a road map of recommended actions to improve port capabilities and readiness to defend against cyberattacks; (CSC Ernesto Ballesteros)**
- **Develop template position (job) announcements with recommended hiring prerequisites and preferences for various levels of port cybersecurity personnel; (Kevin Clement, Chris Wolski)**
- **Create a template for a periodic port cybersecurity report modeled after Texas' BOSA (Joel Aud, CSA Jerrel Conerly)**

1530 – Brief Backs

1600 – Close

2024 Port Cybersecurity Workshop

APPENDIX- CYBER ASSETS

TASK: Create an Appendix for Port Security Plans of contacts to Federal, State, and Regional cybersecurity assets and intelligence agencies;

An objective of the Port Cybersecurity Workshop is to identify and physically meet available federal, state, and regional cybersecurity assets who may assist ports in cyber assessments, preparedness, protection, response, and recovery efforts. Port Security Personnel will establish formal (preferred) and alternate lines of communications with each.

To this end, each port security officer will complete the information below during the course of the Workshop, a copy of which can then be placed in Port Response Plans.

APPENDIX TBD: Federal, State and Regional Cyber Assets

Listed below are Federal, State, and Regional cyber assets with purview in port cybersecurity operations, who may assist ports in cyber preparedness, protection, response, and recovery efforts. Preferred and alternate lines of crisis communications are identified.

FEDERAL

- **U.S. Coast Guard** (USCG). Coast Guard cyber assets with immediate purview over Port insert name are:

  Office Title:
  Name (*last updated insert date*):
  Telephone:
  Alternate Telephone:
  Email:
  Alternate Email:
  Mailing Address:

  Physical Address:

  Preferred Method of Crisis Communications:

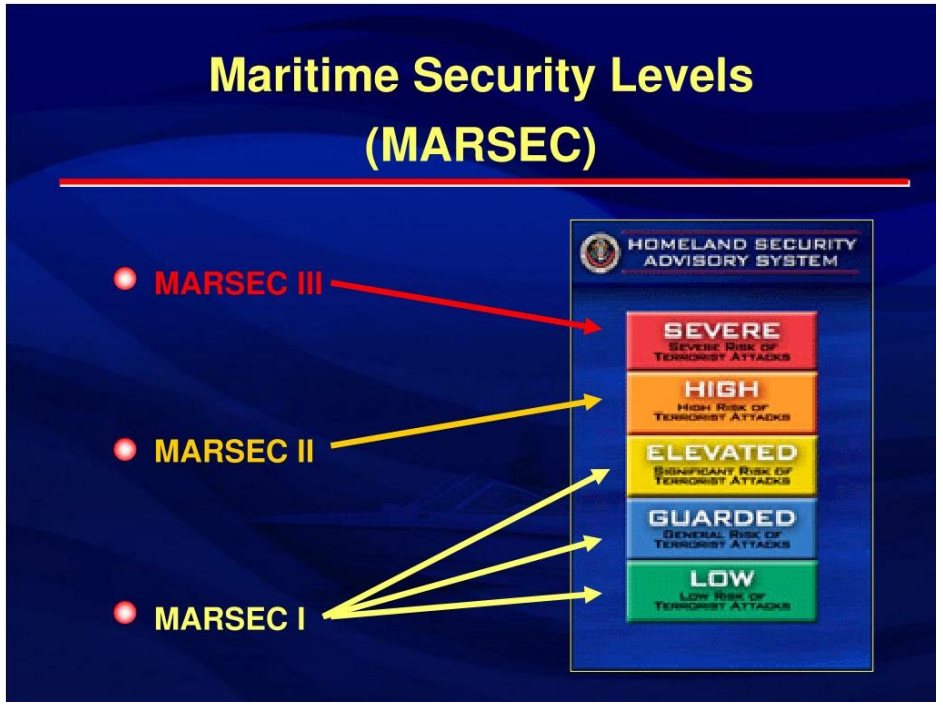
- **Cybersecurity and Infrastructure Security Agency** (CISA). Cybersecurity Advisor(s) with purview over Port insert name are:

  Office Title:

2024 Port Cybersecurity Workshop

WORKSHOP EXERCISE DOCUMENTATION

TASK: Identify recommended cybersecurity actions to be performed at various MARSEC levels;



Facilitators:

Chris Wolski,
Sean Plankey,

2024 Port Cybersecurity Workshop

WORKSHOP EXERCISE DOCUMENTATION

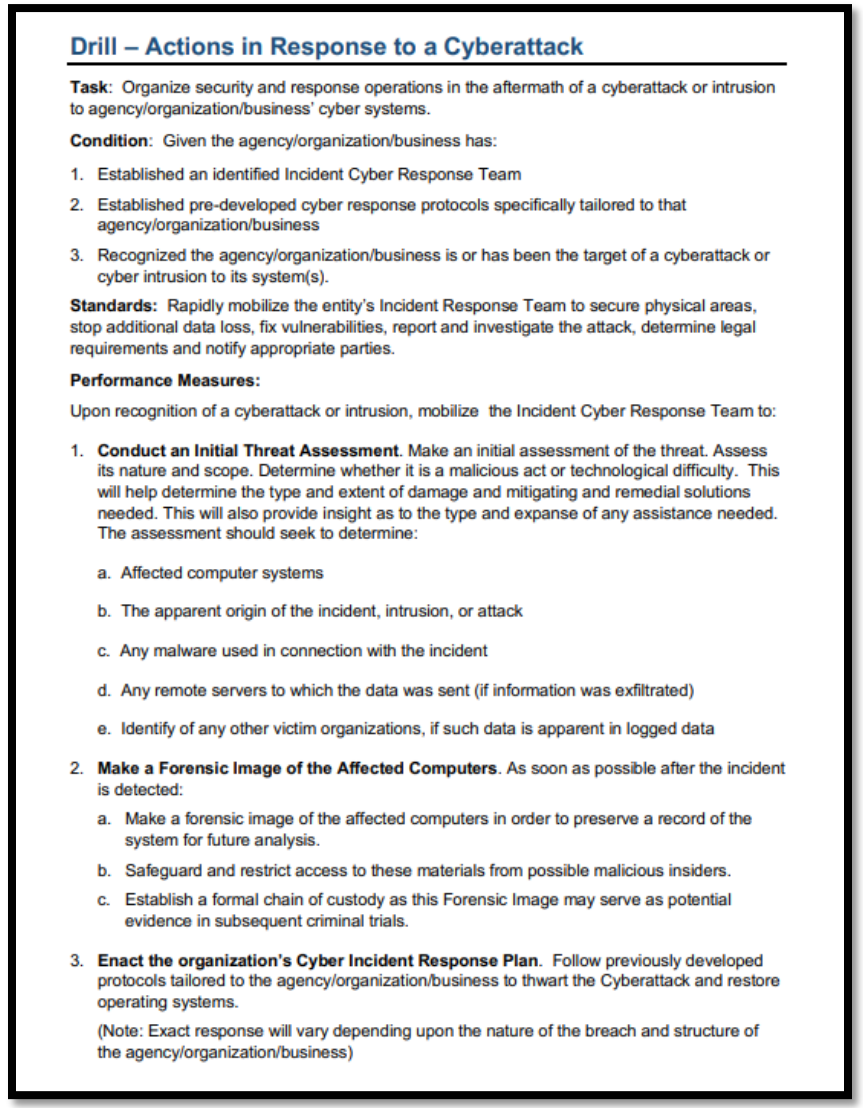
TASK: Create a Port protocol for response to a cyber intrusion and/or attack;

Facilitators:

CSA George Reeves

Jennifer Marusak

CSA Todd Vasilou



Drill – Actions in Response to a Cyberattack

Task: Organize security and response operations in the aftermath of a cyberattack or intrusion to agency/organization/business' cyber systems.

Condition: Given the agency/organization/business has:

1. Established an identified Incident Cyber Response Team
2. Established pre-developed cyber response protocols specifically tailored to that agency/organization/business
3. Recognized the agency/organization/business is or has been the target of a cyberattack or cyber intrusion to its system(s).

Standards: Rapidly mobilize the entity's Incident Response Team to secure physical areas, stop additional data loss, fix vulnerabilities, report and investigate the attack, determine legal requirements and notify appropriate parties.

Performance Measures:

Upon recognition of a cyberattack or intrusion, mobilize the Incident Cyber Response Team to:

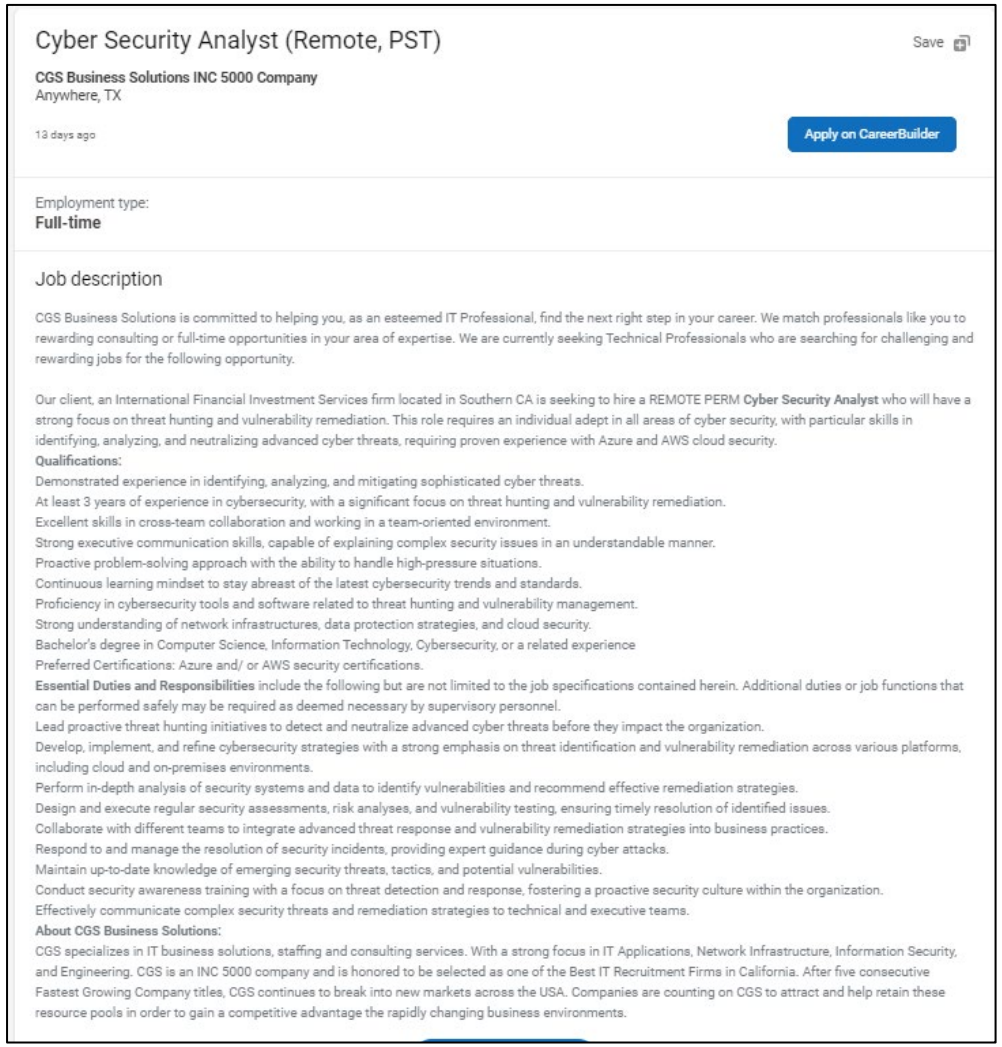
1. **Conduct an Initial Threat Assessment**. Make an initial assessment of the threat. Assess its nature and scope. Determine whether it is a malicious act or technological difficulty. This will help determine the type and extent of damage and mitigating and remedial solutions needed. This will also provide insight as to the type and expanse of any assistance needed. The assessment should seek to determine:
   a. Affected computer systems
   b. The apparent origin of the incident, intrusion, or attack
   c. Any malware used in connection with the incident
   d. Any remote servers to which the data was sent (if information was exfiltrated)
   e. Identify of any other victim organizations, if such data is apparent in logged data
2. **Make a Forensic Image of the Affected Computers**. As soon as possible after the incident is detected:
   a. Make a forensic image of the affected computers in order to preserve a record of the system for future analysis.
   b. Safeguard and restrict access to these materials from possible malicious insiders.
   c. Establish a formal chain of custody as this Forensic Image may serve as potential evidence in subsequent criminal trials.
3. **Enact the organization's Cyber Incident Response Plan**. Follow previously developed protocols tailored to the agency/organization/business to thwart the Cyberattack and restore operating systems.

   (Note: Exact response will vary depending upon the nature of the breach and structure of the agency/organization/business)

2024 Port Cybersecurity Workshop

WORKSHOP EXERCISE DOCUMENTATION

TASK: Develop template position (job) announcements with recommended hiring prerequisites and preferences for various levels (entry, manager) of port cybersecurity personnel.



Cyber Security Analyst (Remote, PST)

Save

CGS Business Solutions INC 5000 Company
Anywhere, TX

13 days ago

Apply on CareerBuilder

Employment type:
Full-time

Job description

CGS Business Solutions is committed to helping you, as an esteemed IT Professional, find the next right step in your career. We match professionals like you to rewarding consulting or full-time opportunities in your area of expertise. We are currently seeking Technical Professionals who are searching for challenging and rewarding jobs for the following opportunity.

Our client, an International Financial Investment Services firm located in Southern CA is seeking to hire a REMOTE PERM **Cyber Security Analyst** who will have a strong focus on threat hunting and vulnerability remediation. This role requires an individual adept in all areas of cyber security, with particular skills in identifying, analyzing, and neutralizing advanced cyber threats, requiring proven experience with Azure and AWS cloud security.

Qualifications:

Demonstrated experience in identifying, analyzing, and mitigating sophisticated cyber threats.
At least 3 years of experience in cybersecurity, with a significant focus on threat hunting and vulnerability remediation.
Excellent skills in cross-team collaboration and working in a team-oriented environment.
Strong executive communication skills, capable of explaining complex security issues in an understandable manner.
Proactive problem-solving approach with the ability to handle high-pressure situations.
Continuous learning mindset to stay abreast of the latest cybersecurity trends and standards.
Proficiency in cybersecurity tools and software related to threat hunting and vulnerability management.
Strong understanding of network infrastructures, data protection strategies, and cloud security.
Bachelor's degree in Computer Science, Information Technology, Cybersecurity, or a related experience
Preferred Certifications: Azure and/ or AWS security certifications.

Essential Duties and Responsibilities include the following but are not limited to the job specifications contained herein. Additional duties or job functions that can be performed safely may be required as deemed necessary by supervisory personnel.

Lead proactive threat hunting initiatives to detect and neutralize advanced cyber threats before they impact the organization.
Develop, implement, and refine cybersecurity strategies with a strong emphasis on threat identification and vulnerability remediation across various platforms, including cloud and on-premises environments.
Perform in-depth analysis of security systems and data to identify vulnerabilities and recommend effective remediation strategies.
Design and execute regular security assessments, risk analyses, and vulnerability testing, ensuring timely resolution of identified issues.
Collaborate with different teams to integrate advanced threat response and vulnerability remediation strategies into business practices.
Respond to and manage the resolution of security incidents, providing expert guidance during cyber attacks.
Maintain up-to-date knowledge of emerging security threats, tactics, and potential vulnerabilities.
Conduct security awareness training with a focus on threat detection and response, fostering a proactive security culture within the organization.
Effectively communicate complex security threats and remediation strategies to technical and executive teams.

About CGS Business Solutions:

CGS specializes in IT business solutions, staffing and consulting services. With a strong focus in IT Applications, Network Infrastructure, Information Security, and Engineering. CGS is an INC 5000 company and is honored to be selected as one of the Best IT Recruitment Firms in California. After five consecutive Fastest Growing Company titles, CGS continues to break into new markets across the USA. Companies are counting on CGS to attract and help retain these resource pools in order to gain a competitive advantage the rapidly changing business environments.

Facilitators:

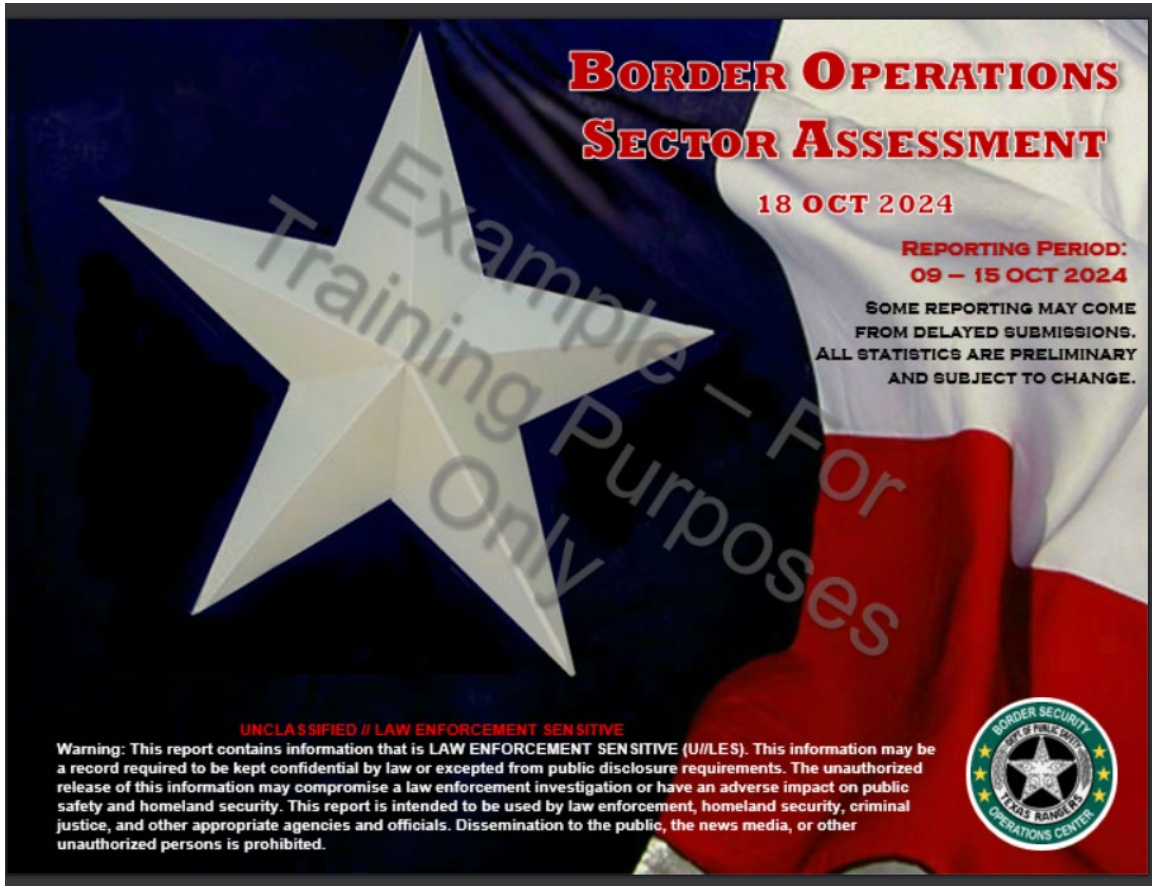
Chris Wolski,

Kevin Clement, BTI Institute

2024 Port Cybersecurity Workshop

WORKSHOP EXERCISE DOCUMENTATION

TASK: Create a template for a periodic port cybersecurity report modeled after Texas' weekly Border Operations Security Assessment (BOSA)



Facilitators:

Joel Aud, BTI Institute

Eric Garcia, Texas Office of Homeland Security

2024 Port Cybersecurity Workshop

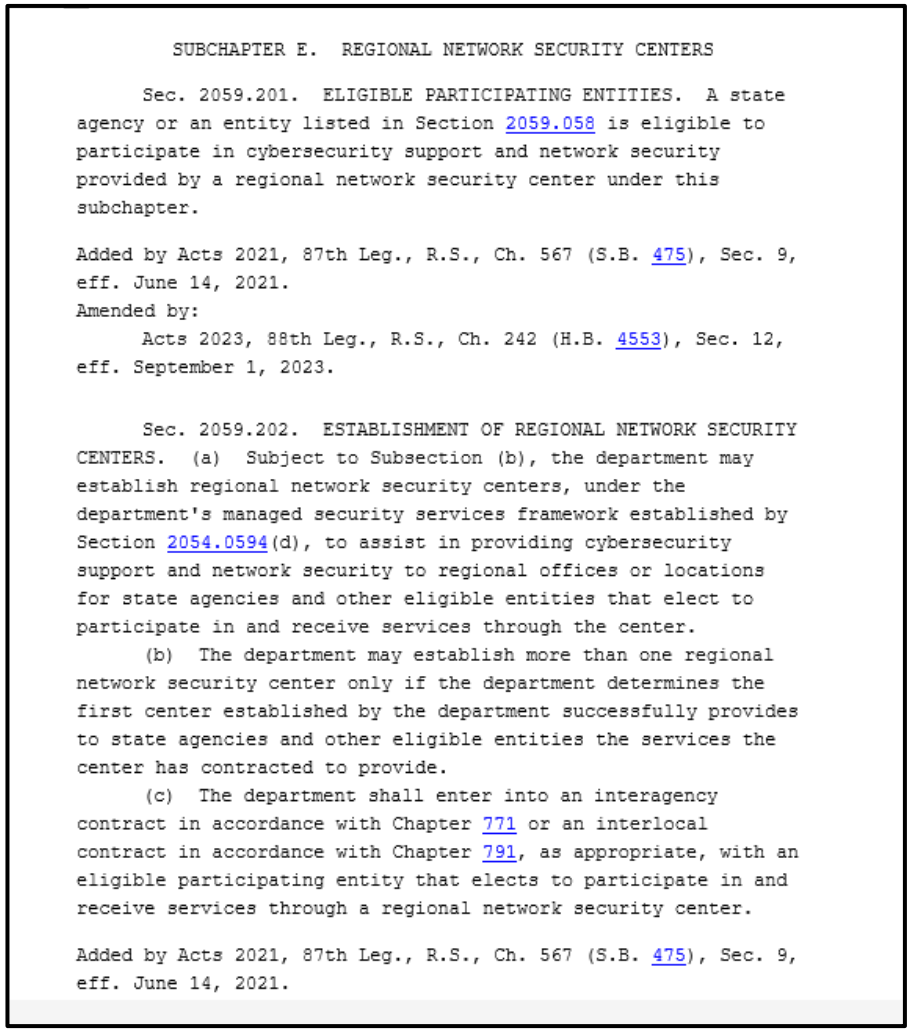
WORKSHOP EXERCISE DOCUMENTATION

TASK: Draft legislation for the creation of Port Cyber Resilience Center(s) as used in Europe and at Port Los Angeles.

Facilitators:

Kevin Clement, BTI Institute

Jonathan King, DIR



SUBCHAPTER E. REGIONAL NETWORK SECURITY CENTERS

Sec. 2059.201. ELIGIBLE PARTICIPATING ENTITIES. A state agency or an entity listed in Section 2059.058 is eligible to participate in cybersecurity support and network security provided by a regional network security center under this subchapter.

Added by Acts 2021, 87th Leg., R.S., Ch. 567 (S.B. 475), Sec. 9, eff. June 14, 2021.
Amended by:
Acts 2023, 88th Leg., R.S., Ch. 242 (H.B. 4553), Sec. 12, eff. September 1, 2023.

Sec. 2059.202. ESTABLISHMENT OF REGIONAL NETWORK SECURITY CENTERS. (a) Subject to Subsection (b), the department may establish regional network security centers, under the department's managed security services framework established by Section 2054.0594(d), to assist in providing cybersecurity support and network security to regional offices or locations for state agencies and other eligible entities that elect to participate in and receive services through the center.

(b) The department may establish more than one regional network security center only if the department determines the first center established by the department successfully provides to state agencies and other eligible entities the services the center has contracted to provide.

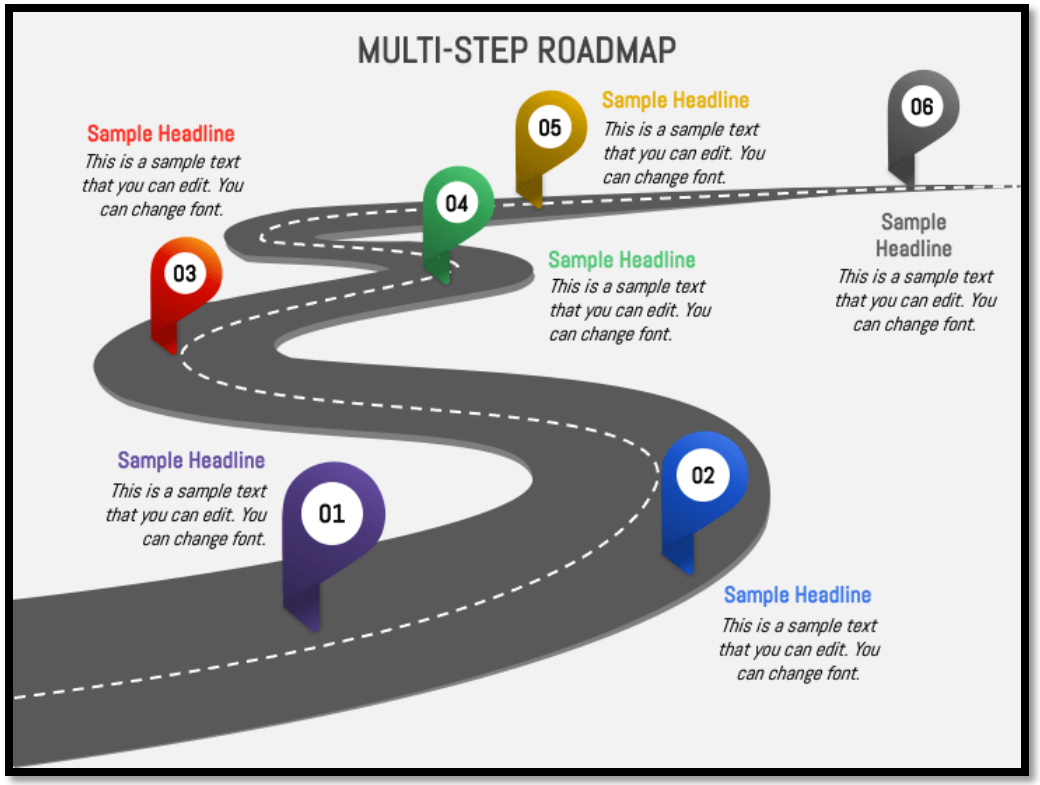
(c) The department shall enter into an interagency contract in accordance with Chapter 771 or an interlocal contract in accordance with Chapter 791, as appropriate, with an eligible participating entity that elects to participate in and receive services through a regional network security center.

Added by Acts 2021, 87th Leg., R.S., Ch. 567 (S.B. 475), Sec. 9, eff. June 14, 2021.

2024 Port Cybersecurity Workshop

WORKSHOP EXERCISE DOCUMENTATION

TASK: Develop a road map of recommended actions to improve ports capabilities and readiness to defend against cyberattacks;



Facilitators:

CSC Ernesto Ballesteros

BTI Institute
Borders • Trade • Immigration
A Department of Homeland Security Center of Excellence

QUESTIONS?