



**#NHCPC24**

**NATIONAL HEALTHCARE COALITION  
PREPAREDNESS CONFERENCE**

*Visions of Progress: Sustainable Strategies for  
Emergency Preparedness & Resilience*

Presented By:



**MESH**

**SAFEGUARDING HEALTHCARE  
COALITIONS AND HEALTHCARE DELIVERY  
A Comprehensive Approach to Cybersecurity**

**GARRETT HAGOOD**  
**Chief Information Security Officer**  
Coastal Bend Regional Advisory Council

**DAVID MERRITT**  
**Region 3 & 4 Emergency Manager**  
New Mexico Healthcare Coalition




**JACK DIMPSEY III**  
**Technical Planning Coordinator**  
Oklahoma State Department of Health  
Emergency Preparedness & Response Service



# TALON CWG OPERATIONAL STRATEGY

## CONSEQUENCE MANAGEMENT

*Consequence management occurs through the consideration of the wider ramifications of an extended downtime event on regional healthcare delivery. This approach moves the focus from the specific hospital victim, to broader consequences that may affect patient care delivery in the region if there is a catastrophic degradation of patient care regionally or nationally.*

-  Large healthcare systems affected by a cyber-attack that have a significant market footprint in your area
-  3rd Party providers to the health sector affected by a cyber-attack cause cascading disruptive effects to many competing hospitals
-  Cyber-attack on power grid and/or water distribution systems that affect healthcare critical infrastructure in your region, triggering hospitals to initiate continuity plans for backup power and water



**TALON**  
CYBER WORKING GROUP

**#NHCPC24**



# MEDICAL ESSENTIAL ELEMENTS OF INFORMATION

## mEEI

*Any critical medical intelligence information required by reporting agencies that collect, analyze, and disseminate EEIs to create situational awareness for the emerging event*

- 🔒 mEEIs are specific to a health sector cyber event that may trigger a regional or national disruption of patient care
- 🔒 The Cyber EEIs are written out in advance as questions by consumers of the EEI information
- 🔒 Expressing complex medical intelligence requirements as a collection of essential elements of information provides the ability of healthcare response stakeholders to create situational reports to support health sector response activities







**TALON**  
CYBER WORKING GROUP

#NHCPC24



# REGIONAL EXTENDED DOWNTIME EEIS

-  **Is the affected hospital(s) diverting/evacuating patients to other healthcare facilities within the regional healthcare delivery system? Is the affected hospital(s) considering extended diversion and/or evacuation?** *(To include forecasted disruption in healthcare delivery in the next 24-48hrs)*
-  **Are sufficient local, regional medical transportation systems in service to accommodate patient diversion and placement to other healthcare facilities in the region?** *(To include forecasted availability of medical transportation in the next 24-48hrs)*
-  **Can the regional healthcare delivery system absorb patient care in critical medical service areas such as Emergency Care, Surgery, Cardiac Care, Stroke Care, Burn Care, Trauma Care, Cancer Care, Dialysis Care, Pediatric Care, Labor & Delivery, and Imaging Diagnostics?** *(To include forecasted disruption of healthcare delivery in the next 24-48hrs)*
-  **Are there any other concurrent operational issues that could affect the regional healthcare delivery systems ability to care for diverted patients from affected hospital(s)?** *(Severe weather, nursing strike, higher than normal census, pandemic medical surge, mass casualty event, staffing shortage etc. To include forecasted disruption of healthcare delivery in the next 24-48hrs)*



# EEIs WE ARE NOT TRACKING

- 🔒 Exposure of personally identifiable information that may result in HIPAA violations on the victim hospital(s)
- 🔒 CMS regulatory issues that may require enforcement actions on the victim hospital(s)
- 🔒 FDA regulatory issues that may require enforcement actions on the victim hospital(s)
- 🔒 Details of the cyber criminal's tactics, techniques and procedures
- 🔒 Details of mitigation strategies that the victim hospital is deploying. Disabling VPNs, remote access, and single sign-in services



**TALON**  
CYBER WORKING GROUP

#NHCPC24



# REASONABLE WORST CASE SCENERIO

**So, let's talk about what could happen. The scenario that we will discuss in the following slides are what we consider a possible and reasonably worst-case scenario of a major incident that affects approximately 25% of your region's bed capacity.**

**WHILE LISTENING  
CONSIDER THE FOLLOWING QUESTIONS**

**How would your HCC respond?**

**What resources does your region have for movement of many patients?**

**What if this incident occurs during a severe weather event, flu season, nursing strike, large special event, or a mass casualty incident?**



**TALON**  
CYBER WORKING GROUP

**#NHCPC24**



# SCENARIO

In today's digital age, where technology is integral to healthcare operations, the importance of robust cybersecurity cannot be overstated. Cyber threats are evolving, and our healthcare infrastructure is a prime target. A breach can not only disrupt services but also compromise patient safety and public trust.



TALON

CYBER WORKING GROUP

#NHCPC24



# RIO GRANDE VALLEY

## Metropolitan Statistical Area

1,300,000 People United States

1,400,000 People Mexico

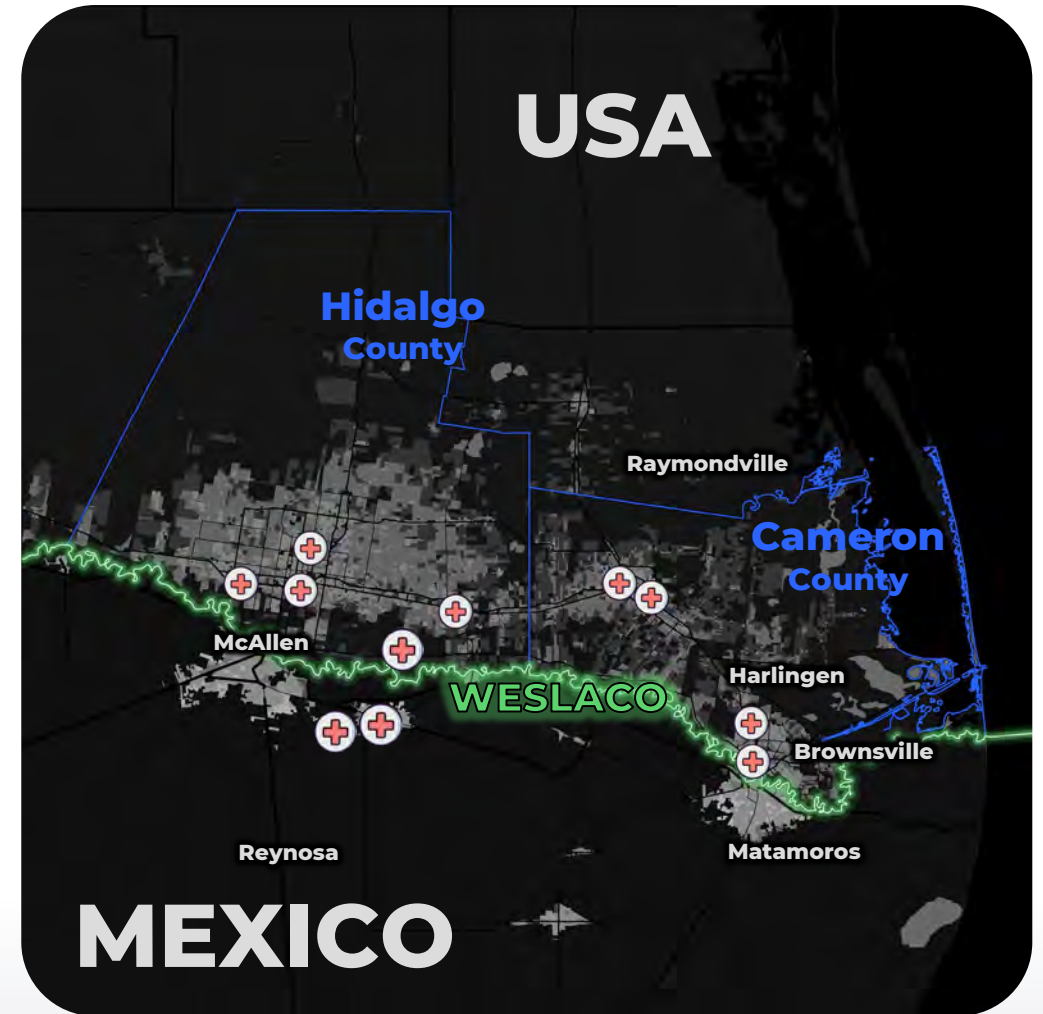
2,700,000 Total Population

## 12 Hospitals

2 Level I Trauma Hospitals

~ 2,700 Licensed Beds

102°F / 84°F Average Summer Temperature



**TALON**  
CYBER WORKING GROUP

#NHCPC24





# SETTING THE STAGE

105°F

Heat Index

95%

2,500 of 2,700 Beds

Bed Capacity



TALON  
CYBER WORKING GROUP

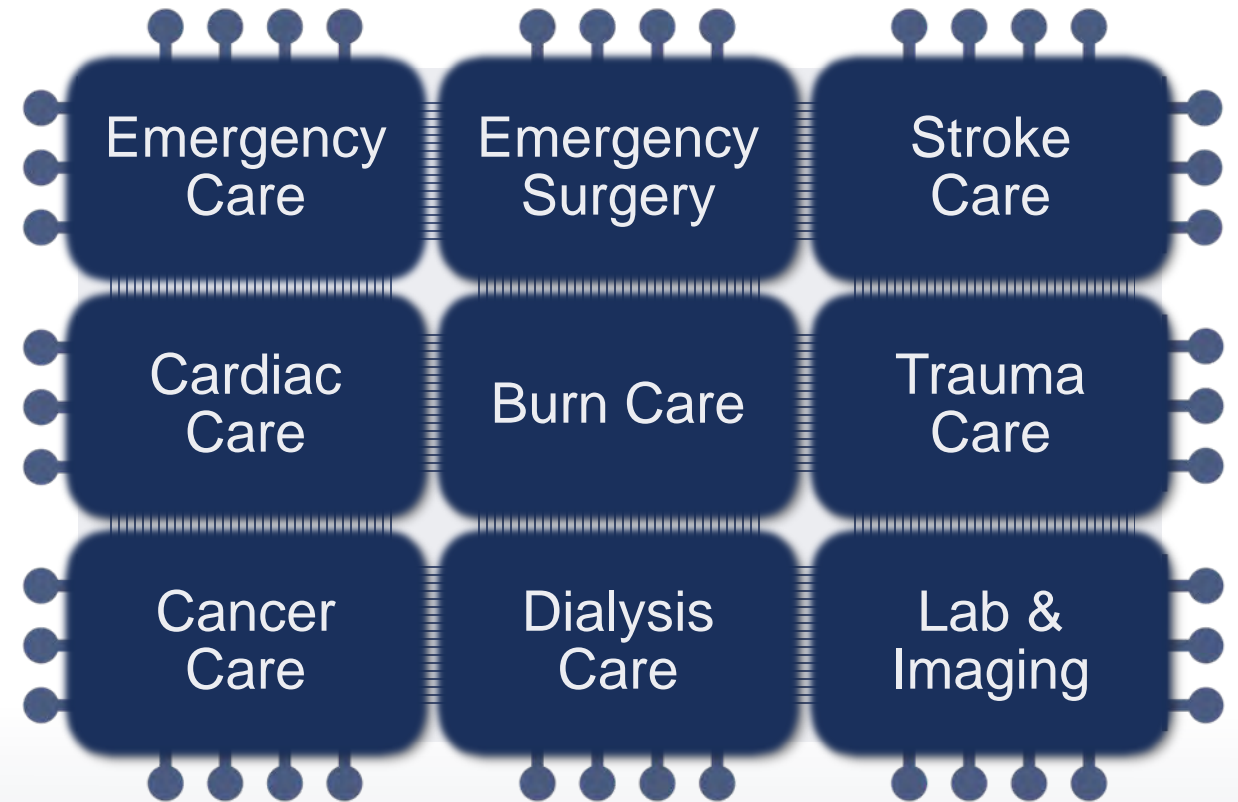
#NHCPC24



# REGIONAL HEALTHCARE DELIVERY

**What types of patient care are disrupted?**

**(mEEI) Can the regional healthcare delivery system (other hospitals) absorb patient care diverted from the targeted hospital(s)?**



**TALON**  
CYBER WORKING GROUP

**#NHCPC24**



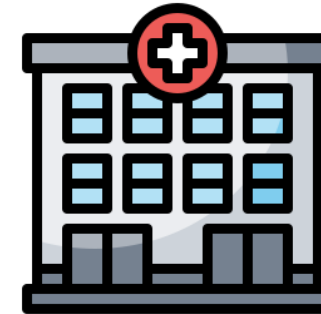
# CONCURRENT ISSUES

- 🔒 **Successful cyber-attacks on healthcare were up 25% during pandemic**
- 🔒 **Cyber-attacks and severe weather are the most concerning combination events to hospital emergency managers**
- 🔒 **(mEEI) Are there concurrent operational issues that could affect the regional healthcare delivery systems ability to care for diverted patients from affected hospital(s)?**

Severe Weather

Nursing Strike

Mass Casualty Event



Higher Than Normal Census

Pandemic Surge

Staffing Shortage



**TALON**  
CYBER WORKING GROUP

**#NHCPC24**



# SETTING THE STAGE

<b>HVAC</b>	Hospital abruptly lost access to function of HVAC / Chiller systems throughout the hospital. All other systems are functioning normally.	Upon assessment, the SCADA systems that control all HVAC / Chillers have been encrypted and are not functional. The vendor notified the facility that full replacement with new equipment would take approximately 3 days.	<b>SCADA</b>
<b>UTILITIES</b>	Upon review of systems all utilities, generators, and electrical functions are normal, but HVAC / Chillers are not functioning.	No manual controls for the complex HVAC / Chiller systems. Temperatures inside the hospital is rising at a rate of 15 degrees / hour from a starting average internal temperature of 71 degrees.	<b>TEMP</b>
		Threat actor is asking for 15 million in crypto for decryption keys. The decision was made to pay... but even with keys technical issues prevented restoration of system and the complex environmental system were permanently damaged from the improper shutdown and loss of cooling. Timeline for HVAC / Chiller repair is approximately 15 – 20 days.	<b>RANSOM</b>



# MEDICAL TRANSPORTATION

- 🔒 Are there enough medical transportation assets available to transport diverted patients to other facilities?
- 🔒 Is diverted patient flow distributed evenly to available receiving facilities?
- 🔒 Does EMS know that the hospital may be experiencing an extended downtime event and may be on divert longer than usually expected?
- 🔒 (mEEI) Is the affected hospital(s) diverting/evacuating patients to other healthcare facilities within the regional healthcare delivery system? Is the affected hospital(s) considering extended diversion and/or evacuation?
- 🔒 (mEEI) Are sufficient local, regional medical transportation systems in service to accommodate patient diversion and placement to other healthcare facilities in the region?



# HOSPITAL DIVERSION / EVACUATION

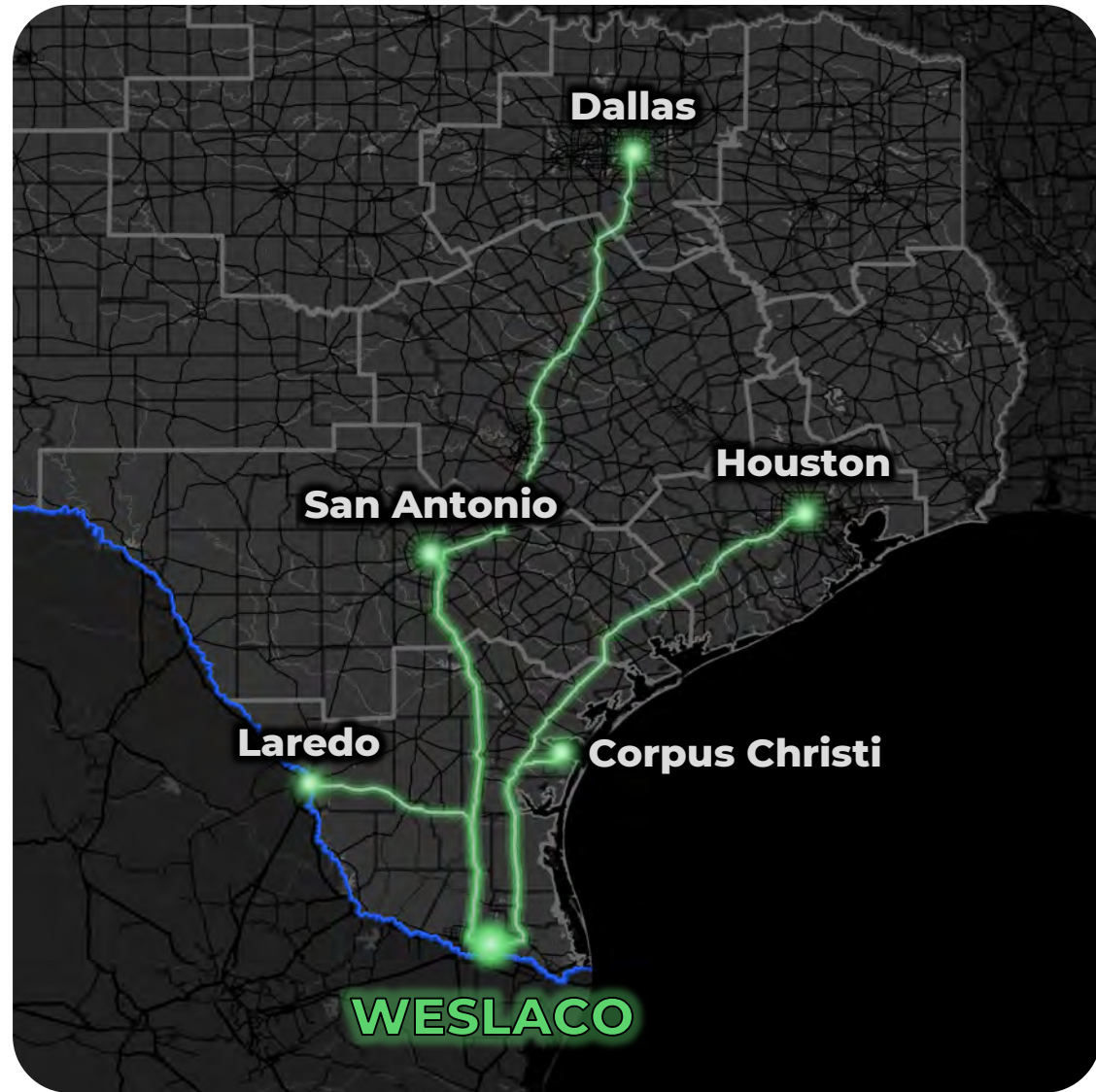
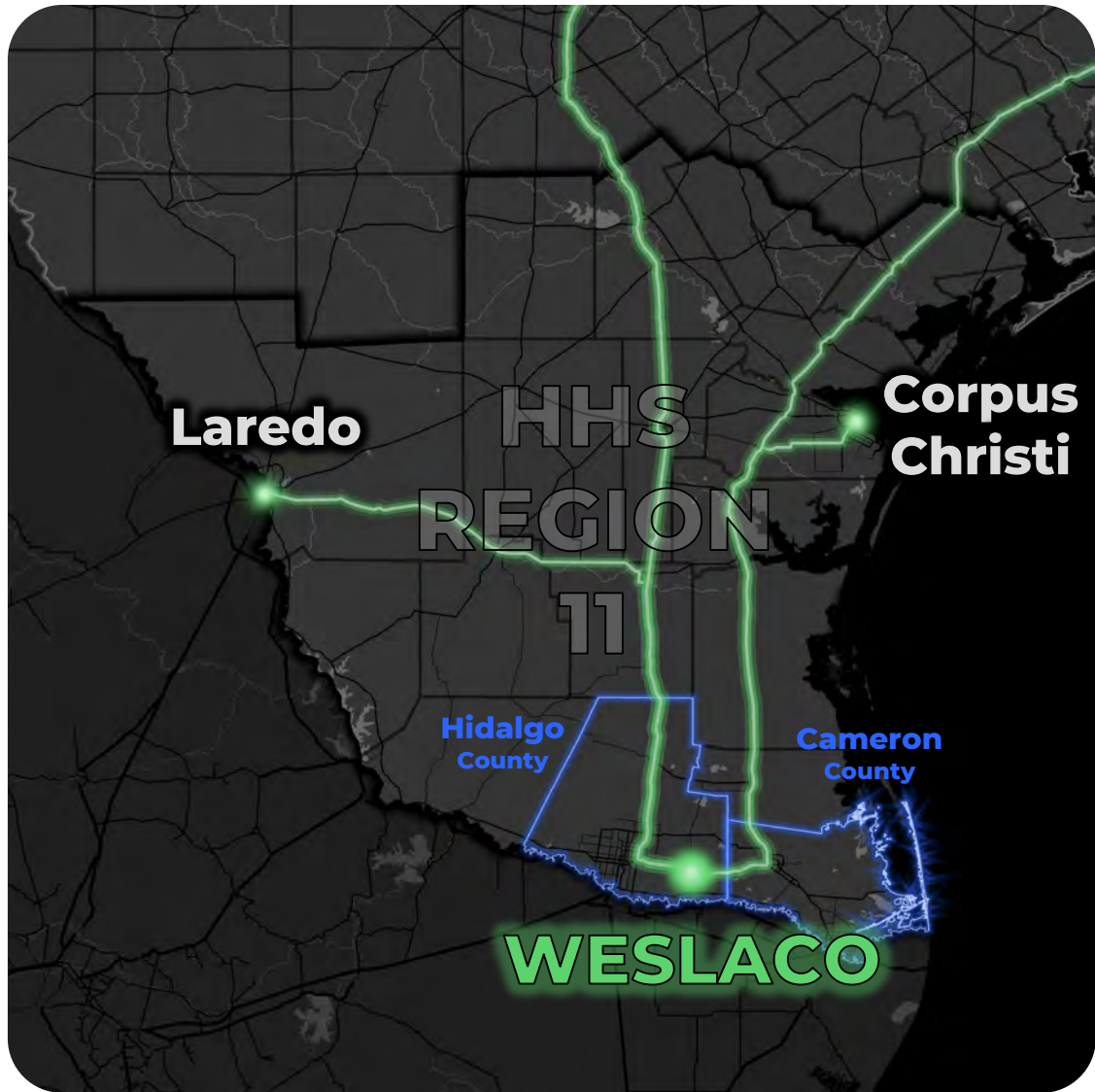
- 🔒 May be difficult to assess how long the hospital will be on diversion at the beginning of the event
- 🔒 Monitoring the affected hospital status, in the beginning, is crucial even if they activate their continuity plan, decompress patient load, and implement downtime procedures
- 🔒 Is this cyber event impacting hospital critical infrastructure, power, and/or water distribution?
- 🔒 (mEEI) Can the regional healthcare delivery system absorb patient care in critical medical service areas such as Emergency Care, Surgery, Cardiac Care, Stroke Care, Burn Care, Trauma Care, Cancer Care, Dialysis Care, Pediatric Care, Labor & Delivery, and Imaging Diagnostics?



**TALON**  
CYBER WORKING GROUP

**#NHCPC24**





# EVACUATION TIMES FROM WESLACO



Discharge

<10% of Patients



Ambulance  
**TRIP TIME**

**CC:** 2 hr  
**LAR:** 3 hrs  
**SA:** 4 hrs  
**HOU:** 6 hrs  
**DAL:** 9 hrs

**CAPACITY 2**



Rotor Wing  
**TRIP TIME**

**CC:** 1 hr  
**LAR:** 1 hr  
**SA:** 2 hrs  
**HOU:** 2 hrs 30 mins

**CAPACITY 1**



Fixed Wing  
**TRIP TIME**

**CC:** 1 hr  
**LAR:** 1 hr  
**SA:** 2 hrs  
**HOU:** 2 hrs 30 mins  
**DAL:** 4 hrs

**CAPACITY 1-2**



AMBUS  
**TRIP TIME**

**CC:** 4 hrs  
**LAR:** 3 hrs  
**SA:** 5 hrs  
**HOU:** 8 hrs  
**DAL:** 11 hrs

**CAPACITY ~20**



**TALON**  
CYBER WORKING GROUP

*The medical one-way transport times displayed are estimates based on typical travel conditions and may vary due to weather, traffic, airspace restrictions, or patient acuity. Capacity limits and trip durations are subject to change depending on resource availability and real-time operational circumstances.*

**#NHCPC24**





# EVACUATING 25% OF THE REGIONS BED CAPACITY

## Worst Case Scenario

- 🔒 Loss of facility function
- 🔒 Compromise to patient and staff safety
- 🔒 The dreaded cyber/physical sentinel event

## Minimize Patient Risk

- 🔒 Early identification and communication of the incident
- 🔒 Quick implementation of extended downtime procedures and other relevant critical response plans
- 🔒 Up-to-date and trained / exercised response plans



# WHAT CAN WE DO?



**TALON**  
CYBER WORKING GROUP

**#NHCPC24**



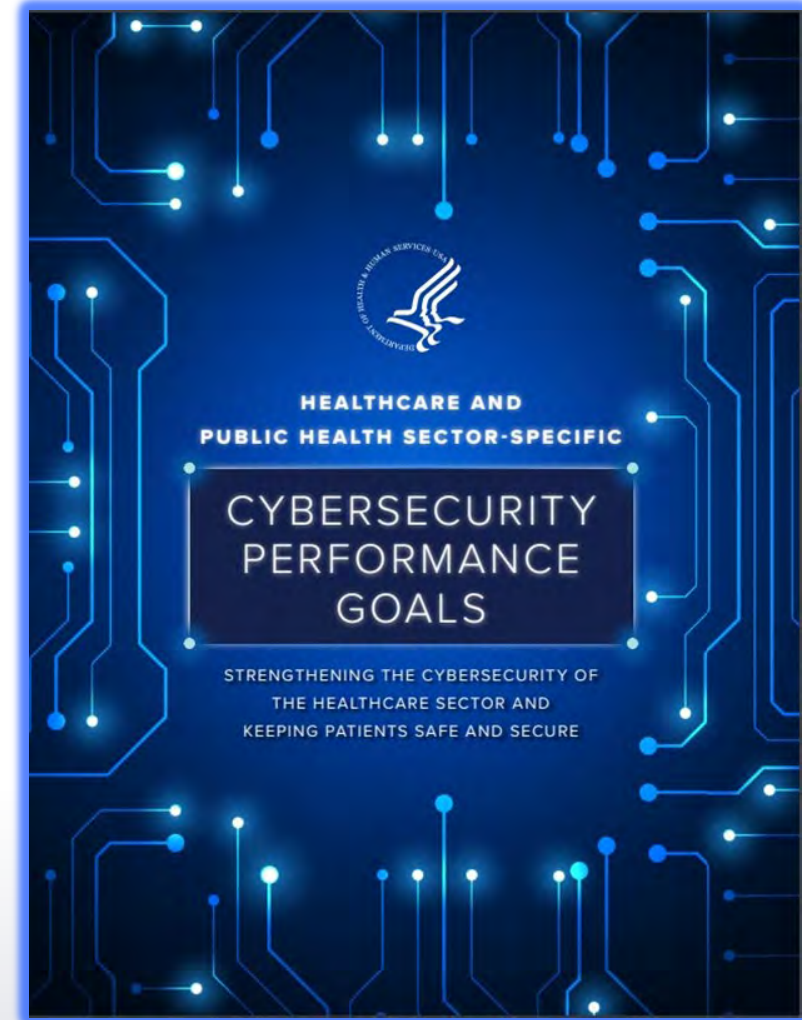
# CYBERSECURITY PERFORMANCE GOALS

## ESSENTIAL GOALS

help healthcare organizations address common vulnerabilities by setting a floor of safeguards that will better protect them from cyberattacks, improve response when events occur, and minimize residual risk.

## ENHANCED GOALS

help healthcare organizations mature their cybersecurity capabilities and reach the next level of defense needed to protect against additional attack vectors.



**TALON**  
CYBER WORKING GROUP

**#NHCPC24**



# CYBERSECURITY PERFORMANCE GOALS

<b>ESSENTIAL GOALS</b>	
<b>Mitigate Known Vulnerabilities</b>	<b>Revoke Credential for Departing Workforce Members</b>
<b>Email Security</b>	Basic Incident Planning & Preparedness
<b>Multifactor Authentication</b>	<b>Unique Credentials</b>
Basic Cybersecurity Training	<b>Separate User &amp; Privileged Accounts</b>
<b>Strong Encryption</b>	<b>Vendow / Supplier Cybersecurity Requirements</b>



# INFORMATION SHARING

**The best way to understand the threat, is to get involved!**

## **MS-ISAC** **FREE**

- 🔒 SLTT Government
- 🔒 <https://learn.cisecurity.org/msisac-registration>

## **Public Safety Threat Alliance** **FREE**

- 🔒 EMS, Law Enforcement, Fire, Emergency Management, PSAP's, FSLTT Government
- 🔒 <https://namrinfo.motorolasolutions.com/join-the-psta>

## **Health-ISAC**

- 🔒 Nominal Fee
- 🔒 <https://health-isac.org/join-h-isac/>

## **CISA Cyber Intelligence Center HSIN COI** **FREE**

- 🔒 Critical Infrastructure CISO / CSO / CIOs and SLTT Government
- 🔒 <https://www.dhs.gov/how-join-hsin>

## **InfraGard** **FREE**

- 🔒 All 16 Critical Infrastructure Sectors
- 🔒 <https://www.infragard.org>

## **HHS CIP Email Distribution List** **FREE**

- 🔒 <https://stg-aspr.hhs.gov/cip/Pages/CIPInquiry%20Form.html>

## **Fusion Center Liaison Programs** **FREE**

- 🔒 <https://www.dhs.gov/fusion-center-locations-and-contact-information>

## **EMR-ISAC HSIN COI** **FREE**

- 🔒 Law Enforcement, EMS, Fire, Emergency Management
- 🔒 <https://www.dhs.gov/emergency-services>



**TALON**  
CYBER WORKING GROUP

**#NHCPC24**



# TRAINING OPPURTUNITIES

## Personal Training

- 🔒 ISC2 CC – Certified in Cybersecurity
- 🔒 TALON CWG Webinars (Coming Soon!)
- 🔒 Health Sector Coordinating Council
- 🔒 Emergency Services Sector Coordinating Council

## Coalition Training

### **TEEX – CDP**

- 🔒 Information Security for Everyone
- 🔒 Understanding Targeted Cyber Attacks
- 🔒 Cybersecurity Risk Awareness for Officials and Senior Management
- 🔒 Demystifying Cyber Attacks
- 🔒 Cybersecurity Incident Response and Management



**TALON**  
CYBER WORKING GROUP

**#NHCPC24**



# HOW TO GET DHS/FBI INVOLVED

## HOW TO BRING HEALTHCARE IT/IS TO THE TABLE AND GET CISA/FBI INVOLVED IN YOUR COALITION

- 🔒 Coordinate with DHS Cybersecurity Advisors and Protective Security advisors to conduct a webinar for your coalition. If you don't know your CSA/PSA <https://www.cisa.gov/audiences/find-help-locally>
- 🔒 Work with your CSA/PSAs to determine if an in-person meeting would be beneficial to your region and invite your regional IT/IS personnel.
- 🔒 Contact your regional FBI Field Office and ask for the Private Sector Coordinator (every FBI field office has one) and ask for a virtual introduction meeting to discuss the purpose and function of your HCC.
- 🔒 Depending on your regional hazards and threats (large chemical plants or petrochemical some coalitions may want to consider engaging with CISA's Chemical Security Inspectors and FBI's Weapons of Mass Destruction Coordinators to discuss healthcare specific capabilities and responses to major incidents. (I know this is not related to Cyber, but it is a way to build a relationship with DHS/FBI)



**TALON**  
CYBER WORKING GROUP

**#NHCPC24**



# HEALTH SECTOR COORDINATING COUNCIL

## INCIDENT RESPONSE & BUSINESS CONTINUITY WORKING GROUP

- 🔒 **Tactical Crisis Response Guide (HIC-TCR)**
- 🔒 **Matrix of Information Sharing Organizations (HIC-MISO)**
- 🔒 **Coordinated Healthcare Incident Response Plan (CHIRP)**
- 🔒 **Operational Continuity – Cyber Incident (OCCI)**
- 🔒 **Healthcare Executive Checklist for Cyber Incidents**
- 🔒 **Cyber Incident Response – Executive Checklist**



Healthcare & Public Health  
Sector Coordinating Councils  

---

**PUBLIC PRIVATE PARTNERSHIP**

<https://www.healthsectorcouncil.org>



**TALON**  
CYBER WORKING GROUP

**#NHCPC24**





# OPERATIONAL CONTINUITY CYBER INCIDENT (OCCI) CHECKLIST

This OCCI Checklist aims to provide organizations of all sizes with key actionable and vetted steps that can be implemented at the first sign of a cybersecurity incident.



## ACTION DRIVEN

Provides operational tasks for the first 0-8 hours of an incident.



## SCALABLE

Applicable for all healthcare settings.

Critical Access  
to  
Large Health Systems



## ROLE-BASED

Aligned with the hospital incident command system.



**TALON**  
CYBER WORKING GROUP



Healthcare & Public Health  
Sector Coordinating Councils  
**PUBLIC PRIVATE PARTNERSHIP**

**#NHCPC24**



# OCCI ELEMENTS



**Editable Collection of Incident Response Guides**



**Priority actions for the first 8 hours of a large-scale Cyber Security Event**



**Actionable items that allows HICS respond quickly**

Version 2.0 released soon through a partnership between HSCC and 405(d) Program and HHS

Version 3.0 will also be released soon and is a printable operational document that can be filled out and provide areas for written notes

Response Guideline	
Cybersecurity/Technology System Prolonged Massive Disruption or Outage	
<i>This checklist outlines recommended initial (first 12 hours) actions and considerations during cybersecurity incidents</i>	
Command positions should be activated as they are needed. If a command position is not activated, actions fall to the incident Commander and can be delegated as appropriate. Position activation may depend on staff availability or the size and scope of the incident.	
Based on assessment by CIO, CISO, and senior leadership, incident command may be activated Threshold for activation:	
<b>A prolonged massive disruption</b> meets or has the potential to meet any of the following:	
a. Patient safety and/or member service impacts	
b. Large-scale clinical workflow, patient care, and/or member service impacts	
c. Implementation of preventative defenses that could impact clinical workflow	
Incident Commander	
Role: Provides overall strategic direction on all site-specific response actions and activities.	
1.1	Identify Incident scope and obtain situational awareness <ul style="list-style-type: none"><li>Identify Scope – One site/multiple sites/Isolated outage/full network outage<ul style="list-style-type: none"><li>Assume it is a malicious (cybersecurity) incident until proven otherwise</li></ul></li><li>Situational awareness – operational, business, and clinical impacts</li></ul>
1.2	Establish a cadence and process for coordination with IS/IT and Cyber Security <ul style="list-style-type: none"><li>Consider command center coordination or unified command based on organizational structure (<i>Hospital, IS/IT, and Cybersecurity Command</i>)</li></ul>
1.3	Activate applicable continuity and downtime plan(s) <ul style="list-style-type: none"><li>If plans do not exist or are not functional, rapidly identify critical services and create a plan to continue/sustain services</li></ul>
1.4	Communicate activation of downtime plans to inform operational changes <ul style="list-style-type: none"><li>Consider use of overhead paging, mass notification system, etc.</li></ul>
1.5	Approve recommendations from Operations relative to: <ul style="list-style-type: none"><li>Scaling services</li><li>Pausing services</li><li>Initiating diversionary status</li></ul>
1.6	Address incident need by activating additional resources
1.7	Understand upstream and downstream impact(s) to partner organizations. Communicate as appropriate. <ul style="list-style-type: none"><li>Community Connect</li><li>Other health systems</li><li>Community partners (e.g., SNF, LTAC, EMS)</li></ul>
1.8	Establish cadence for ongoing impact assessment and briefing (e.g., operational periods)



**TALON**  
CYBER WORKING GROUP



Healthcare & Public Health  
Sector Coordinating Councils  
**PUBLIC PRIVATE PARTNERSHIP**

**#NHCPC24**



# OCCI V3

Response Guideline	
<b>Cybersecurity/Technology System Prolonged Massive Disruption or Outage</b> <i>This checklist outlines recommended initial (first 12 hours) actions and considerations during cybersecurity incidents</i> <i>Please use this workbook and its findings to inform your Incident Action Plan</i>	
<small>Command positions should be activated as they are needed. If a command position is not activated, actions fall to the Incident Commander and can be delegated as appropriate. Position activation may depend on staff availability or the size and scope of the incident.</small>	
Based on assessment by CIO, CISO, and senior leadership, incident command may be activated Threshold for activation: <b>A prolonged massive disruption</b> meets or has the potential to meet any of the following: <ol style="list-style-type: none"> <li>Patient safety and/or member service impacts</li> <li>Large-scale clinical workflow, patient care, and/or member service impacts</li> <li>Implementation of preventative defenses that could impact clinical workflow</li> </ol>	Initially Impacted Systems:
Incident Commander	
<small>Role: Provides overall strategic direction on all site-specific response actions and activities.</small>	
1.1 Identify Incident scope and obtain situational awareness <ul style="list-style-type: none"> <li>Identify Scope – One site/multiple sites/Isolated outage/full network outage               <ul style="list-style-type: none"> <li>Assume it is a malicious (cybersecurity) incident until proven otherwise</li> </ul> </li> <li>Situational awareness – operational, business, and clinical impacts</li> </ul>	<b>Name:</b> <b>Non-VOIP Phone:</b> Assigned to: Time:  Completed by: Time:
1.2 Establish a cadence and process for coordination with IS/IT and Cyber Security <ul style="list-style-type: none"> <li>Consider command center coordination or unified command based on organizational structure (<i>Hospital, IS/IT, and Cybersecurity Command</i>)</li> </ul>	Assigned to: Time:  Completed by: Time:  Where has this cadence been posted?

Operations Section Chief	
<small>Role: Develop and recommend strategies and tactics to continue clinical and non-clinical operations for the duration of the incident response and for recovery.</small>	
<b>Name:</b> <b>Non-VOIP Phone:</b>	
<b>Name:</b> <b>Non-VOIP Phone:</b>	
6.1 Activate downtime procedures <ul style="list-style-type: none"> <li>Identify safe, alternative processes for patient care based on technical outage</li> <li>Initiate downtime processes:               <ul style="list-style-type: none"> <li>Utilize business continuity or downtime computers if available</li> <li>Build paper charts for all patients using information printed from downtime computers or paper downtime forms.</li> <li>Print critical service delivery information (e.g., patient charts, staff schedules, patient schedules)</li> <li>Establish patient and specimen label process</li> </ul> </li> <li>Note: this could be an extended downtime (days or weeks) – address downtime procedures that need to be refined to support extended downtime</li> <li>Establish or implement back charting criteria</li> <li>Deploy strike teams to provide just-in-time training and regulatory requirements on downtime charting and documentation</li> </ul>	Task: Leader Assigned to: Time:  Task: Leader Assigned to: Time:  Task: Leader Assigned to: Time:  Task: Leader Assigned to: Time:  Task: Leader Assigned to: Time:

## Editable and Printable Collection of Incident Response Job Action Sheets

Version 3 (October 2024)

**CONFIDENTIAL**



**TALON**  
CYBER WORKING GROUP



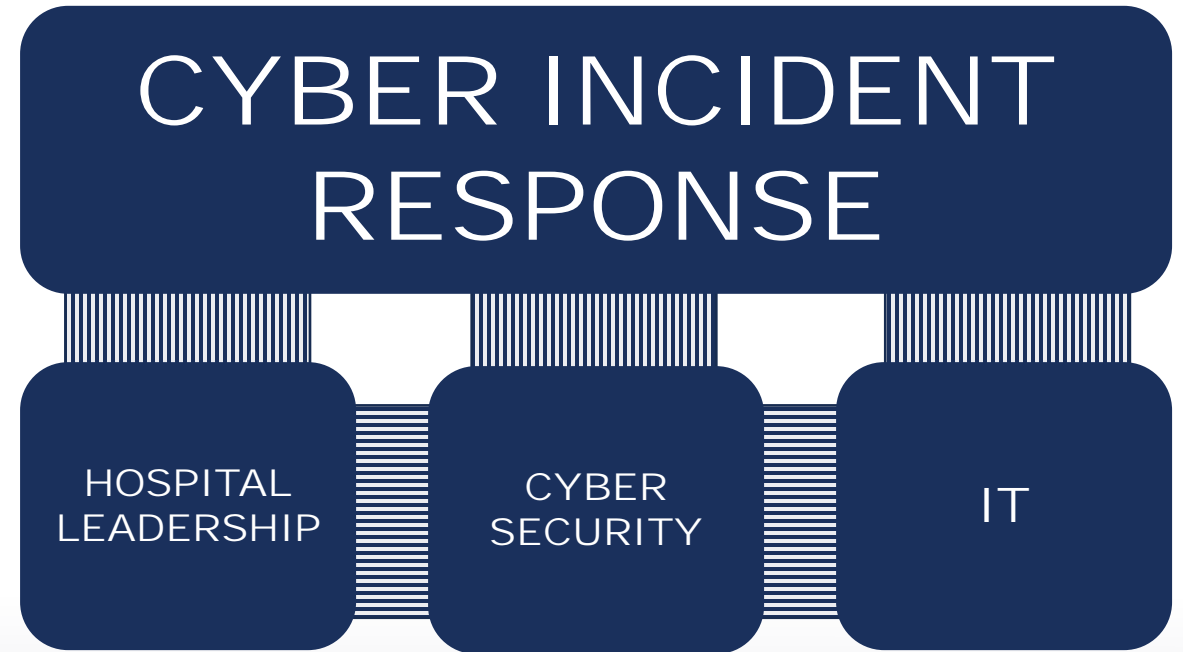
Healthcare & Public Health  
Sector Coordinating Councils  
**PUBLIC PRIVATE PARTNERSHIP**

**#NHCPC24**



# COORDINATED HEALTHCARE INCIDENT RESPONSE PLAN CHIRP

- 🔒 Plan template to guide the response to a large-scale cybersecurity incident
- 🔒 Platform to unite Cyber Security / Information Technology response plans and Hospital EOPs
- 🔒 Leveraged as a stand-alone document or a supporting document to other supplemental plans



**TALON**  
CYBER WORKING GROUP



Healthcare & Public Health  
Sector Coordinating Councils  
**PUBLIC PRIVATE PARTNERSHIP**

**#NHCPC24**



# FROM PANIC TO PLAN

## EXECUTIVE STRATEGIES FOR HANDLING CYBERSECURITY EVENTS

Executive Checklist Outlining key recommendations for hospital executives to effectively prepare for and respond to large-scale cybersecurity attacks

### Incident Response Actions



### Continuity Considerations



### Communication Recommendations



**TALON**  
CYBER WORKING GROUP



Healthcare & Public Health  
Sector Coordinating Councils  
**PUBLIC PRIVATE PARTNERSHIP**

**#NHCPC24**

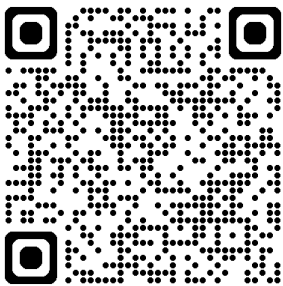


# HEALTH SECTOR COORDINATING COUNCIL

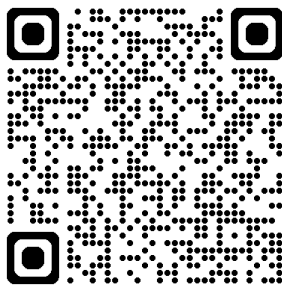
## DOWNLOADABLE RESOURCES



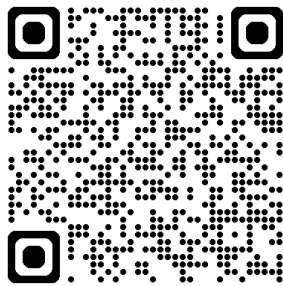
OCCI



CHIRP



CIREC



TALON

CYBER WORKING GROUP



Healthcare & Public Health  
Sector Coordinating Councils

**PUBLIC PRIVATE PARTNERSHIP**

#NHCPC24



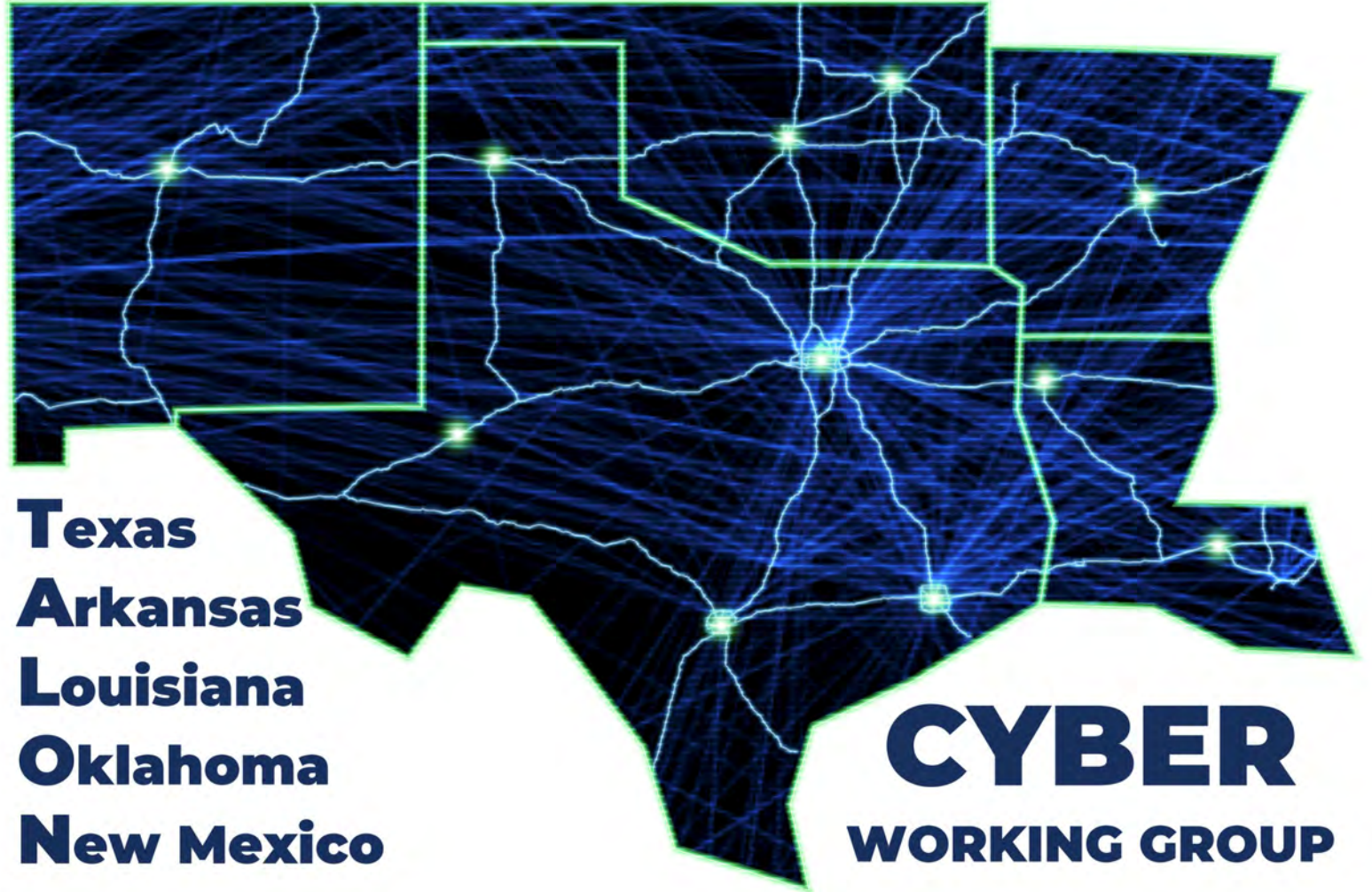
# QUESTIONS?

To be added to our email distribution list, email the TALON Cyber Admin Team at

[intake@r6hppcyber.us](mailto:intake@r6hppcyber.us)

If you are a FSLTT government employee or a HPP Contractor and would like to join our TLP:AMBER TALON CWG Signal chat please email your name, org, and contact info to [intake@r6hppcyber.us](mailto:intake@r6hppcyber.us) to be added.

# TALON



**Texas**  
**Arkansas**  
**Louisiana**  
**Oklahoma**  
**New Mexico**

**CYBER**  
**WORKING GROUP**