# critical infrastructure PROTECTION AND RESILIENCE N. AMERICA

**March 10th-12th, 2026**

Crowne Plaza
BATON ROUGE, LOUISIANA, USA

*A Homeland Security Event*

## Securing the Inter-Connected Society

*For Securing Critical Infrastructure and Safer Cities*

Co-Hosted & Supported by::

International Association of CIP Professionals

INFRAGARD MEMBERS ALLIANCE LOUISIANA

**REGISTER TODAY**
**Early Bird Discount**
**deadline**
**February 10th,2026**

**SPECIAL RATES FOR GOVERNMENT AND OWNER/OPERATORS**
**Register by February 10th**
**see inside for details**

**The ever changing nature of threats, whether natural through climate change, or man-made through terrorism activities, either physical or cyber attacks, means the need to continually review and update policies, practices and technologies to meet these growing demands.**

## Preliminary Conference Programme

**Critical Infrastructure Protection and Resilience North America will bring together leading stakeholders from industry, operators, agencies and governments to debate and collaborate on securing America's critical infrastructure.**

**Register online at www.ciprna-expo.com**

Global Cybersecurity Partner:

ESET Cybersecurity Progress. Protected.

Media Partner:

critical infrastructure PROTECTION AND RESILIENCE NEWS

***Leading the debate for securing America's critical infrastructure***

Supporting Organisations:

INFRAGARD HOUSTON · AUTO-ISAC · Food and Ag ISAC · GBRIA · MARINE EXCHANGE · CAMO · IACI · IT ISAC · LEPA


# Welcome to the 8th Critical Infrastructure Protection and Resilience North America

There are 16 critical infrastructure sectors whose assets, systems, and networks — whether physical or virtual — are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on national security, economic security, public health, or safety.

In 2024, the government adopted a new foundational policy, National Security Memorandum on Critical Infrastructure Security and Resilience (NSM-22), which replaced the previous framework established by Presidential Policy Directive 21 (PPD-21). Under NSM-22, federal departments and agencies — acting as Sector Risk Management Agencies (SRMAs) — are assigned responsibility for managing risk in each of the 16 sectors. The memorandum elevates the role of Cybersecurity and Infrastructure Security Agency (CISA) as the national coordinator for critical-infrastructure security and resilience.

NSM-22 emphasizes the importance of establishing minimum security and resilience requirements for critical infrastructure entities. It calls for effective accountability mechanisms, which may include the use of regulation, federal procurement standards, grants, and financial incentives, to encourage owners and operators to meet or exceed these baseline security standards.

Under NSM-22, federal roles include coordinating cross-sector risk management; enhancing real-time information and intelligence sharing; and promoting investments in technologies and practices that strengthen resilience against evolving threats — from cyberattacks to natural hazards and supply-chain disruptions.

Since the return of the Trump administration in 2025, cybersecurity policy has been reshaped again. In June 2025, a new executive order, Sustaining Select Efforts To Strengthen the Nation's Cybersecurity (EO 14306), amended prior cybersecurity orders and re-emphasized protections for digital infrastructure, cyber resilience, and secure software development. The new order tasks federal agencies — including CISA — with accelerating adoption of stronger security practices, post-quantum cryptography, and modern secure-software development standards.

The 2025 order underlines the need to defend against nation-state cyber threats (notably from countries such as China, Russia, Iran, and North Korea) targeting U.S. systems — including those tied to critical infrastructure. It directs federal departments to harden network security, improve software supply-chain resiliency, and update standards for procurement and operations.

In this updated context, U.S. policy reflects a hybrid approach that combines the structural risk-management framework under NSM-22 with renewed, more technical cybersecurity directives under the new Trump-era order, seeking to defend critical infrastructure against both digital and physical threats in a rapidly evolving threat environment.

**We must be prepared**

We must remain vigilant. The nation's critical infrastructure underpins everyday life — in energy, communications, water, healthcare, transportation, and more — and defending it requires coordinated, updated, and adaptive efforts across government, private sector, and civil society.

Critical Infrastructure Protection and Resilience Americas will bring together leading stakeholders from industry, operators, agencies and governments to collaborate on securing North America.

**Please register online at www.ciprna-expo.com.**

We look forward to welcoming you to Critical Infrastructure Protection & Resilience North America and the Crowne Plaza Executive Hotel, Baton Rouge, LA on March 10th-12th, 2026.

Register online at www.ciprna-expo.com.


# Welcome from the Conference Chairman

Dear Friends and Colleagues,

**Collaborating and Cooperating for Greater Security**

It gives me great pleasure to invite you to join us at the Critical Infrastructure Protection and Resilience North America (CIPRNA) conference in Baton Rouge, Louisiana for what will be 3 days of exciting and informative presentations and discussions on securing North America's critical infrastructure and information.

This is our 8th annual conference here in the United States and follows on from our very successful European event which took place in Brindisi, Italy in October 2025. This year we are delighted to have InfraGard Louisiana as our Co-Hosts and also the support of a number of organisations, which include, The Resiliency Initiative, Auto-ISAC, MarineSafe811, InfraGard Houston and the Coastal and Marine Operators Pipeline Industry Initiative (CAMO Initiative).

There is an exciting line up of topics and expert speakers, as you will see from the very packed agenda, where we will seek to explore the complexities and innovations in place around the protection and resilience of our Critical National Infrastructure and Information.

CIPRNA seeks to bring together leading stakeholders from industry, operators, agencies, academia and government to provide detailed insights into current policy and practices and to collaborate on the efforts required to continually address the range of challenges faced across our critical sectors.

Those challenges are exacerbated by the complexity and interconnected nature of today's global risk landscape and create ever increasing concerns for those within the infrastructure community. Threats and hazards increasingly occur together, they cascade across systems, and amplify one another.

Our societies are facing multiple threats and hazards that are unpredictable, that are new to us and have consequences that may be much broader and deeper than we might imagine.

Geopolitical tensions, climate change, system failures and human error can all lead to the disruption or failure of critical processes which can have major consequences for the functioning of our society.

Those critical processes can be disrupted by deliberate threats emanating from state actors, terrorism, activism and criminal activities. In particular, as we all know, state actors pose an increasing threat to critical infrastructure and information. This threat is apparent in, among other things, an increase in the use of hybrid tools, such as sabotage, espionage, disinformation and of course cyberattacks.

As automation grows at a pace and as the world increasingly relies on interconnected digital systems, the vulnerability of critical infrastructure to cyber risks continue as a pressing concern.

In our endeavours to deal with the range of challenges, across both the physical and cyber spectrums and alongside the increasing scale of natural events and disasters, we have to continually consider our approach to the protection and resilience of our critical entities.

In seeking to explore these issues we have a fantastic agenda lined up with some excellent speakers covering a wide range of important topics and presenting their considered views on the way forward in protecting, securing and developing the resilience of our infrastructure and information internationally.

The conference is specifically designed to stimulate debate and your active participation across the sessions will add real value in the development of new thinking. I know you will find this a most rewarding and enjoyable event and I look forward to seeing you in Baton Rouge.

John Donlon QPM FSyl
Conference Chair

Follow us:

Critical Infrastructure Protection & Resilience


## Why Attend?

Your attendance to Critical Infrastructure Protection and Resilience North America will ensure you are up-to-date on the lastest issues, policies and challenges facing the security of America's critical national infrastructure (CNI).

You will also gain an insight in to what the future holds for North America, the collaboration and support between neighbours required to ensure CNI is protected from future threats and how to better plan, coordinate and manage a disaster.

- High level conference with leading industry speakers and professionals
- Learn from experiences and challenges from the experts
- Gain insight into national CIP developments
- Constructive debate, educational opportunities and cooperation advocacy
- Share ideas and facilitate in valuable inter-agency cooperation
- Exhibition showcasing leading technologies and products
- Networking events and opportunities

For further information and details on how to register visit
www.ciprna-expo.com

For conference or registration queries please contact:
Ben Lane
Event Director
E: benl@torchmarketing.co.uk

## Who Should Attend

Critical Infrastructure Protection and Resilience North America is for:

- Local/State/Federal Police and Security Agencies
- DHS, CISA, FEMA, TSA, DISA, GAO, NSA, NCTC, FBI and related emergency management, response and preparedness agencies
- Emergency Services
- National government agencies responsible for national security and emergency/contingency planning
- Local/State Government
- CEO/President/COO/VP of Operators of national infrastructure
- Security Directors/Managers of Operators of national infrastructure
- CISO of Operators of national infrastructure
- Facilities Managers – Nuclear, Power, Oil and Gas, Chemicals, Telecommunications, Banking and Financial, ISP's, water supply
- Information Managers
- Port Security Managers
- Airport Security Managers
- Transport Security Managers
- Event Security Managers
- Architects
- Civil Engineers
- NATO
- Military
- Border Officials/Coast Guard

***Join us in Baton Rouge, Louisiana for Critical Infrastructure Protection and Resilience North America and join the great debate on securing America's critical infrastructure.***

*"Disruption to infrastructures providing key services could harm the security and economy of North America as well as the well-being of its citizens."*


| Exhibition Opening Hours | | On-Site Registration Hours | |
|---|---|---|---|
| Tuesday March 10th | 1.00pm to 7.30pm | Tuesday March 10th | 8.00am to 6.00pm |
| Wednesday March 11th | 9.00am to 5.30pm | Wednesday March 11th | 8.30am to 5.00pm |
| Thursday March 12th | 9.00am to 4.30pm | Thursday March 12th | 8.30am to 4.00pm |

## REGISTER ONLINE AT WWW.CIPRNA-EXPO.COM

**Register Online Today at www.ciprna-expo.com/register**

**REGISTRATION**

The Critical Infrastructure Protection & Resilience North America is open and ideal for members of local, state and federal government, emergency management agencies, emergency response and local/state/federal law enforcement or inter-governmental agencies, DHS, CISA, FEMA, TSA, DISA, GAO, NSA, NCTC, NSA, FBI, Fire, Police, INTERPOL, AMERIPOL and associated Agencies and members (public and official) involved in the management and protection of critical national infrastructure.

The Conference is a MUST ATTEND for direct employees, CSO, CISO's and security, fire and safety personnel of critical infrastructure owner/operators.

Industry companies, other organizations and research/Universities sending staff members to Critical Infrastructure Protection & Resilience North America are also invited to purchase a conference pass.

**EARLY BIRD DISCOUNT - deadline February 10th, 2026**

Register yourself and your colleagues as conference delegates by February 10th, 2026 and save with the Early Bird Discount. Registration details can be found at www.ciprna-expo.com/register.

**REGISTER ONLINE TODAY AT WWW.CIPRNA-EXPO.COM/REGISTER**

**Discounts for Members of Supporting Associations**

If you are a member of one of the following trade associations, supporters of the Critical Infrastructure Protection & Resilience North America, then you can benefit from a special discount on standard rates:

- INFRAGARD Louisiana and INFRAGARD Houston
- National Security & Resilience Consortium (NS&RC)
- International Association of CIP Professionals (IACIPP)
- International Security Industry Organization (ISIO)
- International Association of Certified ISAOs (IACI)
- Auto ISAC

**Check the Registration Information at www.ciprna-expo.com/registration-fees**


## Schedule of Events

### Tuesday March 10th, 2026

1:00pm - Exhibition Opens

**2:00pm-3:30pm - Opening Keynote**

3:30pm-4:00pm - Networking Coffee Break

4.00pm-5:30pm - Session 1: National & Regional Emergency Management Preparedness

5:30pm - Networking Reception in Exhibition Hall

### Wednesday March 11th, 2026

#### Track One

9:00am-10:30am - Session 2a: Emerging Threats against CI

10:30am-11:15am - Networking Coffee Break

11:15am - 12:30pm - Session 3a: Cybersecurity Regulations, Best Practice and Minimum Standards

12:30pm-2:00pm - Delegate Networking Lunch

2:00pm-3:30pm - Session 4a: Cyber Threats, Cybersecurity and AI in CI

3:30pm-4:15pm - Networking Coffee Break

4:15pm - 5:30pm - Session 5a: Risk Management & Mitigation Strategies

#### Track Two

9:00am-10:30am - Session 2b: Communications Sector Symposium

10:30am-11:15am - Networking Coffee Break

11:15am - 12:30pm - Session 3b: Transport Sector Symposium

12:30pm-2:00pm - Delegate Networking Lunch

2:00pm-3:30pm - Session 4b: Power & Energy Sector Symposium

3:30pm-4:15pm - Networking Coffee Break

4:15pm - 5:30pm - Session 5b: Maritime, Ports and Pipelines Symposium

### Thursday March 12th, 2026

9:00am-10:30am - Session 6a: Strategic Resilience Planning

10:30am-11:15am - Networking Coffee Break

11:15am - 12:30pm - Session 7a: Drones and UAS

9:00am-10:30am - Session 6b: Technologies to Detect and Protect

10:30am-11:15am - Networking Coffee Break

11:15am - 12:30pm - Session 7b: Secure by Design

12:30pm-2:00pm - Delegate Networking Lunch

2pm-3:30pm - Session 8: Collaboration, Information Sharing and Enhancing PPPs

3:30pm-4:00pm - Review, Discussion and Conference Close

4.30pm - Exhibition Close

**Register online at www.ciprna-expo.com/register**


## Tuesday March 10th

# Conference Programme

**2:00pm-3:30pm - OPENING KEYNOTE**

Chair: John Donlon QPM, FSyI
*International adviser on security intelligence*

Steve Casapulla, Executive Assistant Director (EAD) for Infrastructure Security (ISD), Cybersecurity and Infrastructure Security Agency (CISA)

Clay Rives, Director, Mayor's Office of Homeland Security and Emergency Preparedness

Col. Robert Hodges, Deputy Secretary of Public Safety Services, Louisiana State Police

Brian Harrell, Former Assistant Secretary for Infrastructure Protection

Lester Millet III, President, Infragard Louisiana

*3:30pm-4:00pm - Networking Coffee Break*

**4:00pm-5:30pm - Session 1: National & Regional Emergency Management Preparedness**

*Comprehensive efforts need to be undertaken by governmental bodies, operators, private sector entities, and other stakeholders, at both national and regional levels to anticipate, prevent, prepare for, respond to, and recover from incidents that could disrupt the functioning of critical infrastructure systems. From risk assessment and identification of potential threats and hazards, to understanding the vulnerabilities of these systems, and the complex interdependencies and cascading failures among different critical infrastructure sectors, developing comprehensive emergency strategies to mitigate them is key to successful resilience.*

*Chair: John Donlon QPM, FSyI*

Joe Threat, Chief Resilience Officer and Deputy Chief Administrative Officer for Infrastructure, City of New Orleans

**The Challenges of Critical Infrastructure Protection: Lessons of Ukraine** - Oleksandr Sukhodolia, Leading Consultant of Critical Infrastructure Protection Department, The State Service of Special Communications and Information Protection of Ukraine

**Preparing Emergency Management/Responder Facilities to Continue Providing Essential Functions During a Long-Duration, Widespread Power Outage** - Michael Lambert, Emergency Preparedness/Homeland Security Planner, Houston-Galveston Area Council of Governments

**Incident Stories From Peak Season: City Grids and Factory Lines Under Fire** - Charles Everette, Chief Information Security Officer, City of Fort Lauderdale

**Charting An Alternate Path to Achieving State and Local Preparedness** - Ollie Gagnon, Chief Homeland Security Advisor, Idaho National Laboratory

*5:30pm-7:30pm - Networking Reception in Exhibit Hall*

**invited*


# Wednesday March 11th

## Track One

### 9:00am-10:30am - Session 2a: Emerging Threats against CI

*This session investigates the evolving landscape of threats against CI, which include terrorism, insider threats, climate and cyberattacks including the emerging challenges asserted by AI, which necessitate a proactive approach to security. To effectively address these emerging challenges, it is crucial to identify, monitor, and assess their potential impact.*

***Chair:** John Donlon, IACIPP*

Senior Representative, FBI*

Mark Fontenot, ICC Manager, Governor's Office of Homeland Security and Emergency Preparedness

**Senior Representative, Cybersecurity & Infrastructure Security Agency***

**Cybersecurity - Global Trends 2026** - Jean-Ian Boutin, Director of Threat Research, ESET

TBC

*10:30am-11:15am - Networking Coffee Break*

### 11:15am-12:30pm - Session 3a: Cybersecurity Regulations, Best Practice and Minimum Standards

*The threat of cyber-attacks by state actors and hacktivists continues to grow as a threat to cause disruption to our infrastructures. We are behind the curve against the attackers, so developing legal requirements, recommended and best practices, and foundational security controls is important to ensure operators and agencies are meeting expected regulation requirements to prevent a successful attack, or what to do following a cyber breach.*

***Chair:** Mike Echols, Max Cybersecurity*

**Critical Infrastructure Sector implementation of the Cybersecurity Framework** - Ron Martin, Professor of Practice, Capitol Technology University

**Engineering against Digital Risk in CIP Applications: Cyber-Informed Engineering Use Cases** - Megan Culler, Technical Director for Critical Energy Cybersecurity, Idaho National Laboratory

Senior Representative, IT-ISAC*

Deborah Kobza, President, IACI

**Securing US Aviation: What Can We Learn from European Frameworks** - Jack Willis, Vice President, Security Engineering and Northeast US, Bridewell

*12:30pm-2:00pm - Delegate Networking Lunch*

## Track Two

### 9:00am-10:30am - Session 2b: Communications Sector Symposium

*Communications is key to any community and its infrastructure assets has become increasingly threatened. Without communications, business will be lost, and any emergency coordination would be a disaster. The internet has become a vital part of communications for all. Protection of communication assets and their resilience is critical for businesses, government and all sectors of CI.*

**From Design to Deployment: Security Architecture and Operating Models in Utility Private Wireless** - Anuj Kumar, Cybersecurity Manager – Enterprises, Nokia

**Quality at Scale: A New Standard for Reliable, High-Performance Data Centers** - Mike Regan, VP Business Performance , Telecommunications Industry Association (TIA)

**Critical Communication Networks - Keeping the Channels Open** - Graeme Hull, Managing Director, SWISSPHONE LLC

**Enabling Critical Infrastructure Security and Operational Efficiency via Private Cellular AI enabled Telecom Open ISAC and SCADA IO processing Capability** - Brenda Connor, Professor of Practice & Senior Technical Managing Director, Texas Tech University Critical Infrastructure Security Institute

**Incommunicado Island: 18 years of incomplete interoperable communications** - Jeffrey Quinones-Diaz, Consultant, The Consulting Lead LLC

*10:30am-11:15am - Networking Coffee Break*

### 11:15am-12:30pm - Session 3b: Transport Sector Symposium

*The movement of goods and people is vital to a local and national thriving economy. Without a safe, secure and resilient transport network, an economy will crumble. The transport network, from rail, road, air and sea, is at threat from cyber attacks, terrorist threats and natural hazards and its protection and resilience is key for communities and countries to maintain their economies.*

Adam Stahl, Senior Advisor, TSA*

Janet St. John, Director of Cybersecurity, AAR

Faye Francy, Executive Director, Auto-ISAC

**Addressing Emerging Challenges in Alabama's Transportation System** - Tracy Fletcher, Assistant State Maintenance Administrator, Alabama DoT

*12:30pm-2:00pm - Delegate Networking Lunch*


# Wednesday March 11th

## Track One

### 2:00pm-3:30pm - Session 4a: Cyber Threats, Cybersecurity and AI in CI

*The cyber threats to Critical Infrastructure continue to increase at the reward of financial gain or major disruption, where chinks in the armour continue to be exposed by malicious actors. How do we better protect the confidentiality, integrity, and availability of IT and OT systems. What role can AI play in assisting cybersecurity processes?*

Joshua Tannehill, Interim Commander, Cyber Reserve Team, Louisiana State Guard; President Louisiana Chapter, Cloud Security Alliance; VP Louisiana Chapter, InfraGard LA

**Cybersecurity for Water in an Age of Advanced Persistent Threats** - Ymir Vigfusson, CTO, Keystrike

**From Digitalisation to Intelligent Resilience: How AI Is Transforming Cybersecurity and Safety in Critical Infrastructures** - Jalal Bouhdada, CEO, Indurex, Netherlands

**The Sovereign Stack: A New Doctrine for Coordinated Critical Infrastructure Defense Against Nation-State Actors** - Bradley Tenenholtz, Senior Consultant , Splyce Consulting, USA

**AI Agents and Graph Neural Networks: Shaping the Next Era of Operational Technology / Information Technology Resiliency** - Kimberly Guedry, Regional Director for Region 6, CISA & Ricky Armwood, Senior Manager, Deloitte Consulting & Cathy Yin, Manager, Deloitte & Touche, USA

*3:30pm-4:15pm - Networking Coffee Break*

### 4:15pm-5:30pm - Session 5a: Risk Management & Mitigation Strategies

*Risk management and mitigation strategies in critical infrastructure are essential for ensuring uninterrupted essential services. With the nation hosting the 2026 World Cup, this process includes identifying, assessing, and treating risks to vital assets, systems, and networks, as well as large event venues and other crowded places. These high-visibility locations require strengthened protective measures to safeguard attendees and support the resilience of infrastructure operations during this period of increased global attention and significantly elevated activity.*

**Sustaining PNT Systems Beyond A 30-Day GPS Disruption** - Mike Roskind, PNT Program Manager, CISA/ NRMC/Space Systems & Services

**Leveraging Technology for Predictive Infrastructure Planning and Resilience in Critical Infrastructure (CI) Systems** - Robert Stephan, Specialist Executive, Deloitte

**Model Based Systems Engineering (MBSE) Analysis & Update of U.S. Infrastructure Data Taxonomy (IDT) Using U.S. National Critical Functions (NCFs)** - Kirk Moen, INCODE CIPR_WG SE & MBSE Volunteer, Boeing

**Executive Protection: Lessons Learned** - Mike Jackson, President, Elite Edge

## Track Two

### 2:00pm-3:30pm - Session 4b: Power & Energy Sector (Grid Resilience) Symposium

*The energy sector has become the most critical of sectors. Without power, driven by oil, gas and renewable energies, all other CI stops. Recent cyber attacks on the energy sector, as well as natural hazards, from hurricanes in the Gulf to fires in California, gives much room for thought on how we best protect our most vital assets, including IT/OT and SCADA systems. How can we mitigate the impact of an attack or outage on the wider community and society, and build greater grid resilience?*

***Chair:*** *Tommy Waller, President & CEO, Center for Security Policy*

**Addressing Supply Chain Security for Louisiana's Electric Grid** - Eric Skrmetta, Commissioner, Louisiana Public Service

**Protecting Louisiana's Electric Grid is Vital to Homeland Security & National Security** - Raymond Crews, Louisiana Representative

**What does a modern OT Cybersecurity program look like?** - Luke Hebert, Manager of Cyber Engineering, Cybirical

**Leveraging existing resources to bolster physical security** - Gary Stergiades, Security Operations Center (SOC) Chief, GridIntel

*3:30pm-4:15pm - Networking Coffee Break*

### 4:15pm-5:30pm - Session 5b: Maritime, Ports and Pipelines Symposium

*The maritime, ports and pipelines sectors are vital for global trade and energy security. Protecting these systems from physical and cyber threats prevents economic disruption, environmental disasters, and ensures the continuous flow of goods and resources essential for national security and prosperity.*

Mel Carraway, Region 4 Security Director, TSA*

**Securing ONG, Chemicals, and Maritime Critical Infrastructure: Enhancing Resilience in Industrial Control Systems** - Marco Ayala, President, InfraGard Houston

Ed Landgraf, Chairman, Coastal And Marine Operators

Maggie O'Connell, Director of Security, Reliability, and Resilience, Interstate Natural Gas Association of America (INGAA)


# Thursday March 12th

## Track One

### 9:00am-10:30am - Session 6a: Strategic Resilience Planning

*A holistic, long-term approach towards building resilience is required to ensuring the continued functioning of CI, especially when faced with increasing frequency and severity of disruptions. It moves beyond traditional "disaster recovery" to embrace the ability to anticipate, adapt, and transform in the face of a wider range of evolving and interconnected threats, embedding resilience thinking into the core values, policies, and daily operations of critical infrastructure organizations and government bodies.*

**Synergising Critical Infrastructure Protection, Resilience, Cybersecurity and Continuity of Operations to Achieve and Sustain Critical Infrastructure Preparedness –** Jeff Gaynor, President, American Resilience

Andrea Davis, President & CEO, The Resiliency Initiative

**Stakeholder Information Protection and Sharing –** Chris Miller, PCII Program Office Outreach Leader, Cybersecurity & Infrastructure Security Agency

**Building Resilience in Critical Infrastructure** - Glenda Snodgrass, President, The Net Effect, LLC

*10:30am-11:15am - Networking Coffee Break*

### 11:15am-12:30pm - Session 7a: Drones and UAS

*Drones pose a growing threat to critical infrastructure due to their increasing accessibility, manoeuvrability, and payload capacity. They can be used for surveillance, delivering explosives, or causing disruptions. However, drones can also act as a facilitator to protect critical infrastructure. In this session we look into the threat, counter measures and impact drones can induce on CI.*

George Rey, Sector Chief Program - COTS Technology, Infragard LA

**Adapting to Aerial Threats: Scalable Non-Disruptive, Non-Kinetic Counter-UAS Strategies for Critical Infrastructure Resilience -** Danny Rajan, GM USA, D-Fend Solutions

St Charles Parish Police*

Senior Representative, Sentrycs*

*12:30pm-2:00pm - Delegate Networking Lunch*

## Track Two

### 9:00am-10:30am - Session 6b: Technologies to Detect and Protect

*What are some of the latest and future technologies, from ground, land or underwater technologies, access controls, and space based or counter drone systems, to predict or detect the wide range of potential physical and cyber threats to CNI. How is AI being utilised in technology to enhance performance.*

Charles Everett, Field CISO Advisor, ESET

**Detecting the undetectable: overcoming clutter, weather, darkness, and occlusion -** Curtis Walters, VP of Sales - Commercial, Echodyne

**TBC**

*10:30am-11:15am - Networking Coffee Break*

### 11:15am-12:30pm - Session 7b: Secure by Design

*Secure by Design is about embedding security as a non-negotiable quality attribute throughout the entire lifecycle of critical infrastructure, making it inherently more robust, resistant to attack, and capable of recovering quickly from inevitable disruptions. From Threat Modeling and Risk Assessment to Secure Supply Chain, it's making security a foundational characteristic from the initial concept and design phase, through development, deployment, operation, and eventual decommissioning.*

**Importance of Embedding a Holistic Approach to Security and Resilience in the Design of Airport Infrastructure -** Sarah-Jane Prew, Associate Aviation Security Consultant, Arup UK

**Transforming Landscapes. How UK CT policing is supporting Aviation Security -** DS Kirsty Rigg, Counter Weapons Threat Team Lead, National Counter Terrorism Security Office UK

**Embedding Enterprise Cyber Resilience into Critical Infrastructure** - Charles Burton, Information Technology Director, Calcasieu Parish Police Jury

**A Holistic Approach to Securing Critical Infrastructure: Beyond Technology and Tactics** - Ric Everett, Senior Security Consultant, IMEG

*12:30pm-2:00pm - Delegate Networking Lunch*


## Thursday March 12th

**2pm-3:30pm - Session 8: Collaboration, Information Sharing and Enhancing PPPs**

*Information sharing and cooperation is crucial for effective risk management and resilience planning. By fostering collaboration among government, operators, and communities, we can enhance the protection of critical infrastructure. However, barriers to information sharing and cooperation persist, partly due to trust. To overcome these challenges, we must build trust and create a supportive environment that encourages open communication and knowledge exchange.*

*Chair: John Donlon QPM FSyI*

**Navigating CISA: Programs, Services, and Building Strategic Partnerships** - Samuel M. Duchac, Executive Officer, Regional Sector Outreach Coordinator, Regional Training & Exercises Coordinator, Cybersecurity & Infrastructure Security Agency

Lester Millet, President, Infragard LA

**What can the National Weather Service (NWS) do for you? -** Lauren Chandler, Warning Coordination Meteorologist, National Weather Service

**Public Private Partnerships to Increase Community Preparedness- how the CAER group trains and exercises with local emergency management and hazmat teams** - Josie Ross, Emergency Management Officer, City of Henderson

Senior Representative, National Council of ISACs

Questions, Discussion, Round Up and Conference Close by John Donlon QPM, FSyI, Conference Chairman

## Networking Reception

**Tuesday March 10th**
**5.30pm - 7:30pm**
**Exhibition Floor**

We invite you to joins us at the end of the opening day for the Critical Infrastructure Protection & Resilience North America Networking Reception, which will see the CNI security industry management professionals gather for a more informal reception, in a Covid compliant environment.

With the opportunity to meet colleagues and peers you can build relationships with senior government, agency and industry officials in a relaxed and friendly atmosphere.

The Networking Reception is free to attend and open to industry professionals.

We look forward to welcoming you.


## The Venue and Accommodation

**Crown Plaza Baton Rouge**
4728 Constitution Ave
Baton Rouge
LA 70808

Located in the heart of Baton Rouge, just off I-10 and College Drive, Crowne Plaza Executive Center Baton Rouge is 10 minutes from the LSU campus and a short drive from Baton Rouge Metropolitan Airport (BTR). Near top attractions like Downtown Baton Rouge, the Louisiana State Capitol, BREC's Baton Rouge Zoo, the LSU Rural Life Museum, and the Mall of Louisiana, we are the ideal choice for your Baton Rouge adventure.

Host meetings and events in our 18 venues within 32,000 square feet of space. Savor Louisiana flavors at our restaurants. Take a dip in our outdoor pool and stay active in our expansive fitness center. Our pet-friendly, spacious accommodations offer free Wi-Fi with plush bedding to sink into at the end of the day. We are your gateway to the best of Baton Rouge!

For more details on the hotel and online booking visit **www.ciprna-expo.com/accommodation**

## Booking Your Accommodation

Special Room Rate for CIPRNA Delegates – $163 prpn (excl taxes)

Promo Code: '**CIP**'

Book your hotel accommodation at the **Crown Plaza Baton Rouge** at **www.ciprna-expo.com/hotel-booking**

Delegates/attendees can make reservations in the following way:

• Online: Reservations can be made online at www.ciprna-expo.com/hotel-booking

**Click on the link, complete your information and quote Promo Code 'CIP' to get your CIPRNA group booking rate.**

**Special Group Rate ends 17th February**

We look forward to welcoming you to Baton Rouge, LA.


## Why participate and be involved?

Critical Infrastructure Protection and Resilience North America provides a unique opportunity to meet, discuss and communicate with some of the most influential critical infrastructure protection, safer cities and security policy makers and practitioners.

Your participation will gain access to this key target audience:

- raise your company brand, profile and awareness
- showcase your products and technologies
- explore business opportunities in this dynamic market
- provide a platform to communicate key messages
- gain face-to-face meeting opportunities

Critical Infrastructure Protection and Resilience North America gives you a great opportunity to meet key decision makers and influencers.

**www.ciprna-expo.com**

## How to Exhibit

Gain access to a key and influential audience with your participation in the limited exhibiting and sponsorship opportunities available at the conference exhibition.

To discuss exhibiting and sponsorship opportunities and your involvement with Critical Infrastructure Protection & Resilience North America please contact:

**Bruce Bassin**
*Americas*
E: bruce@torchmarketing.co.uk
T: +1 702.600.4651

**Paul Gloc**
*ROW*
E: paulg@torchmarketing.co.uk
T: +44 (0) 7786 270 820

## Sponsorship Opportunities

A limited number of opportunities exist to commercial organisations to be involved with the conference and the opportunity to meet and gain maximum exposure to a key and influential audience.

Some of the sponsorship package opportunities are highlighted here.

- Platinum Sponsor - $19,500
- Gold Sponsor - $15,500
- SIlver Sponsor - $10,950
- Bronze Sponsor - $8,950
- Conference Proceedings Sponsor - $5,950
- Delegate Folder Sponsor - $4,950
- Networking Reception Sponsor - $4,950
- Coffee Break Sponsor - $4,950
- Site Visit & Coach Sponsor - $4,950
- Lanyard Sponsor - $4,950
- Badge Sponsor - $4,950

Packages can be designed and tailored to meet your budget requirements and objectives.
Please enquire for further details.

## Exhibiting Investment

The cost of exhibiting at the Critical Infrastructure Protection & Resilience North America conference is:

**Table Top Exhibit 5'x7' - $3,495**
**Table Top Exhibit 10'x10' - $5,495**
Raw space with 1 x table and 2 x chairs, pipe and drape, electrical socket, wi-fi, 1 Exhibitor Delegate pass (2 for 10x10 booth) with full conference access, lunch and coffee breaks included, listing in the official event guide and website.

**Exhibitors also benefit from a 50% discount on Conference Delegate Fees.**

**ASK ABOUT OUR BOOKING BUNDLES FOR EXTRA EXPOSURE**

**ALL PRICES SUBJECT TO 10.5% BR/LA SALES TAX**


## Sponsors and Supporters:

We wish to thank the following organisations for their support and contribution to Critical Infrastructure Protection & Resilience North America 2026.

Global Cybersecurity Partner:

ESET Cybersecurity Progress. Protected.

Supported & Co-Hosted by:

International Association of CIP Professionals

INFRAGARD MEMBERS ALLIANCE LOUISIANA

Bronze Sponsor:

ECHODYNE

Badge & Coffee Break Sponsor:

AXIS COMMUNICATIONS

Lanyard Sponsor:

CAPITOL Technology University

Supporting Organisations:

INFRAGARD HOUSTON

AUTO-ISAC

IT ISAC

Food Ag ISAC

IACI

GBRIA

LEPA

CAMO

MARINE SAFE

NS&RC

ISIO

Help2Protect

Flagship Media Partner:

critical infrastructure PROTECTION AND RESILIENCE NEWS

Media Supporters:

govCIO OUTLOOK

BIOMETRIC

BORDER SECURITY REPORT

CIOReview

Owned & Organised by:

TORCH


**Participating Organizations Have Included:**


## Highlighted Speakers

**Steve Casapulla**

**Executive Assistant Director (EAD) for Infrastructure Security (ISD), Cybersecurity and Infrastructure Security Agency (CISA)**

Steve Casapulla serves as the Executive Assistant Director (EAD) for Infrastructure Security at the Cybersecurity and Infrastructure Security Agency (CISA). He concurrently serves as the Interim Assistant Director (AD) for the National Risk Management Center (NRMC) and the Acting Chief Strategy Officer at the agency.

Prior to joining CISA, Casapulla was the Director for Critical Infrastructure Cybersecurity in the Office of the National Cyber Director. He previously spent more over a decade at CISA, holding a variety of senior roles, and his prior federal service includes work at the Small Business Administration and Department of State.

Casapulla is an officer in the U.S. Navy Reserves and has made multiple overseas deployments in support of contingency operations and the Global War on Terror.

A graduate of the U.S. Merchant Marine Academy in Kings Point, NY, he has earned graduate degrees from Georgetown University and the Naval War College. He holds a CISM certification and received an Executive Certificate in Public Leadership from the Harvard Kennedy School.

**Colonel Robert P. Hodges**

**Deputy Secretary of Public Safety Services, Louisiana State Police**

Colonel Robert P. Hodges was appointed as the 27th Superintendent of the Louisiana State Police. He also serves as Deputy Secretary of Public Safety Services. This responsibility spans an agency of more than 2700 employees, with a budget of over $635 million and collections of over $2.5 billion in revenue. As Deputy Secretary, he oversees along with the Louisiana State Police, the Office of State Fire Marshal, the Office of Motor Vehicles, the Louisiana Highway Safety Commission, the Louisiana Gaming Control Board, the Liquefied Petroleum Gas Commission, the Office of Legal Affairs, and the Office of Management and Finance.

Colonel Hodges, a native of New Orleans, graduated from Brother Martin High School and earned his Bachelor of Criminal Justice from Louisiana State University, where he was a member of Sigma Nu Fraternity. He began his career with the Louisiana State Police in 1995 as a patrol Trooper assigned to Troop B in New Orleans. Colonel Hodges has held career assignments in both Patrol and Investigations as Trooper, Sergeant, Lieutenant, Captain, and Major. Prior to his appointment, he served as Command Inspector of Region 2 Patrol.

**Brian Harrell**

**Former Assistant Secretary for Infrastructure Protection, DHS**

Brian currently serves as the Vice President and Chief Security Officer (CSO) for a large energy company with assets and operations in 25 states. He is responsible for the company's physical and cybersecurity, privacy, intelligence, and business continuity units.

In 2018, Brian was appointed by the President of the United States to serve as the sixth Assistant Secretary for Infrastructure Protection, at the Department of Homeland Security. Brian also served as the first Executive Assistant Director for Infrastructure Security at the U.S. Cybersecurity and Infrastructure Security Agency (CISA).

Brian has spent time during his career in the US Marine Corps and various private sector agencies with the goal of protecting the United States from security threats.


**Euclid Talley**

Assistant Director, Governor's Office of Homeland Security and Emergency Preparedness (GOHSEP)

Euclid Talley's current assignment is as Assistant Director for Security and Interoperability, working for the Governor's Office of Homeland Security and Emergency Preparedness, managing critical infrastructure protection, cyber security, criminal intelligence, emergency communications, and the Louisiana Center for Safe Schools. He provides oversight for vulnerability threat assessments and security protection planning to critical infrastructure of national interest e.g. national defense, national security, or national resource protection. Additional areas of responsibility include Overseeing and safeguarding information, personnel, property, assets, and/or material from theft, loss, misuse, fraud, disclosure, espionage, sabotage, or terrorism.

He has four years of military service managing Human Resources, Officer Recruiting, and Career Management for a force of 9,000+ Soldiers, including medical doctors, dentists, lawyers, and mental health providers, along with basic combat and combat support branches.

Euclid also has eight years of military service assigned as the WMD Consequence Manager, responding to emergency incidents and providing direct support to Federal/State and civilian authorities conducting counter-terrorism to CBRNE events. Areas of responsibility included providing identification, mitigation, lab analysis, evidence preservation, intelligence analysis, physical security to special events, and force protection. He handled all natural and manmade Disaster Recovery projects and provided POTUS Protection in support of the Secret Service Hazardous Materials Mitigation Unit during multiple events.

He also has ten years of military assignments assigned as the Construction Project Management and Engineering Operations Program Management for critical infrastructure rebuild and force protection projects in support of Operation Freedom's Sentinel- Afghanistan and Operation Iraqi Freedom. Assigned as Construction Project Management for projects valued over $28M. Managed Natural Disaster Recovery and Force Protection Engineer Construction projects, e.g., Honduras, Belize, Norway, and CONUS, in support of civilian and military authority.

**Lester Millett III**

**InfraGard Louisiana President And Port Of South Louisiana Safety Risk Agency Manager**

InfraGard Louisiana President and Port of South Louisiana Safety Risk Agency Manager Lester Millet III was recently awarded the 2020 Government Technology & Services Coalition Homeland Security Today Citizen of Mission Award. The award goes to an individual who devotes personal time, energy and resources to work for causes related to homeland security. Volunteers, nonprofit leaders, corporate employees and others are eligible for nomination as long as they devote time and effort to supporting the homeland mission.

**Kimberly Guedry**

**Regional Director for Region 6, Cybersecurity and Infrastructure Security Agency (CISA)**

Kimberly Guedry serves as the Regional Director for Region 6 of the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). Headquartered in the Dallas-Fort Worth Metroplex, Region 6 serves public and private sector partners across Arkansas, Louisiana, New Mexico, Oklahoma, and Texas to better understand, manage, and reduce risk to cyber and physical infrastructure, building a more secure and more resilient Nation.

Prior to leading CISA Region 6, Ms. Guedry served as Director of Analytic Capability at CISA's National Risk Management Center. Akin to Chief Information Officer, she led end-to-end building of analytic models, methods, and data and their integration into risk analysis tools to support CISA and its partners in managing cyber and physical risks to our Nation's critical infrastructure.


**Eric Skrmetta**

**Commissioner, Louisiana Public Service**

Commissioner Skrmetta has saved ratepayers over $8 billion since taking office, reducing residential utility rates to the lowest in the nation. He has ushered in new power plants to build Louisiana's energy efficiency and independence. He improved water systems, demanded transparency on consumer billing, protected Louisiana communities by ensuring prison telephone calls remain monitored, reduced storm recovery costs, and returned over a half billion dollars in rate credits to Louisiana consumers. He is also the first Public Service Commissioner in the nation to have proposed and passed a directive that orders the state's grid operators to cease purchasing, and including, any foreign produced devices in electric utilities from hostile adversaries, such as the People's Republic of China.

**Raymond Crews**

**Louisiana Representative**
**Member of Select Committee on Homeland Security, LA**

Raymond is a Christian Conservative that strongly believes in both social and fiscal conservative issues. He believes that the right to life starts at conception, defending the 2nd Amendment of the US Constitution, religious freedom for all people, and that building a strong economy starts with creating an environment where small businesses can thrive. Raymond is a combat pilot who served our country in the United States Air Force for 17 years. He is a small business owner with experience in Aerial Mapping and Energy Consulting and he currently serves on four vital committees in the Louisiana Legislature:
Labor and Industrial Relations, Chair
Health and Welfare
House Select Committee on Homeland Security
Special Committee on Military and Veterans Affairs

**Tommy Waller**

**President & CEO, Center for Security Policy**

Lt. Col. Tommy Waller, USMC Ret is the President and CEO of the nonprofit Center for Security Policy. Waller retired from the Marine Corps Reserves at the rank of Lieutenant Colonel after serving more than two decades on both active duty and in the reserves with deployments to Afghanistan, Iraq, Africa, and the Caribbean. His last military assignment was as the Commander of the Marine Corps Reserve's only Force Reconnaissance Company. While in the Corps, he graduated from the Marine Corps Command and Staff College and was cross assigned to serve as a key staff member of the U.S. Air Force's Electromagnetic Defense Task Force (EDTF). During his decade of civilian service to the Center for Security Policy he has led the nationwide "Secure the Grid Coalition," helping inspire policies to secure this most critical infrastructure at the federal, state, and local levels. Waller holds a BA in International Relations from Tulane University, New Orleans, LA and was the first recipient of the Captain Robert M. Secher Scholarship to the Wharton School of Business where he completed an executive education course on high stakes negotiations.


**Tracy Fletcher**

Assistant State Maintenance Administrator, Alabama Department of Transportation

Tracy Fletcher serves as the Assistant State Maintenance Administrator for the Alabama Department of Transportation (ALDOT), where she oversees the state's Emergency Management responses and leads the Workforce Safety Program.

A graduate of Auburn University at Montgomery with a bachelor's degree in international economics, Tracy brings 26 years of experience in highway construction and maintenance operations to her role.

Her career began in the private sector, where she spent a decade working on construction projects, gaining extensive experience in project management. She later joined ALDOT, starting in the construction section before transitioning into maintenance operations, where she has continued to advance her leadership and expertise.

**Oleksandr Sukhodolia**

**Leading Consultant of Critical Infrastructure Protection Department, The State Service of Special Communications and Information Protection of Ukraine**

Oleksandr Sukhodolia works at the National Institute for Strategic Studies of Ukraine and takes position of a Head of Critical Infrastructure Protection, Energy and Ecological Security Department. He is also Leading Consultant of Critical Infrastructure Protection Department, The State Service of Special Communications and Information Protection of Ukraine.

Oleksandr Sukhodolia has extensive experience in public service and higher education. Since 1998, he has been working on issues of energy security at different positions at governmental agencies. Currently his research interests focused on the energy security, critical infrastructure security and resilience. Oleksandr has led the development of the Law of Ukraine "On Critical Infrastructure" (2021) and later contributed to drafting the regulatory acts to implement provision of the Law. O.Sukhodolia co-authored the books, namely: "Developing the critical infrastructure protection system in Ukraine" (2017), "Organizational and legal aspects of ensuring the security and resilience of Ukraine's critical infrastructure" (2019), "Energy Security of Ukraine: Methodology of System Analysis and Strategic Planning" (2021). Oleksandr holds a Ph.D degree in Electrical Engineering and Dr. (Habil) in Public Administration.

**Anuj Kumar**

**Senior Security Architect, Nokia**

Anuj Kumar is a distinguished technology executive with over 15 years of experience in the telecommunications industry. He specializes in empowering Communication Service Providers (CSPs) globally to securely design, optimize, and scale their core network infrastructures and business operations systems. His expertise encompasses a broad spectrum of critical telecom domains, including:

• 5G Service-Based Architecture; • 4G-LTE; • IMS VoLTE; • Subscriber Data Management (SDM); • Online Charging Systems (OCS); • Policy Management (PCRF); • Broadband and Fiber Operations; • 5G/ Private 5G Monetization

Before joining Nokia, Anuj Kumar held several key leadership positions in the telecom and IT sectors. Notably, he served as a Core Solution Consultant at Salesforce, where he spearheaded 5G Monetization and BSS transformation initiatives for telecommunications customers across North America, driving transformation in their sales and support channels.


**Benjamin Lampe**

**Engineer, Idaho National Laboratory**

Mr. Benjamin Lampe is an Engineer and Researcher at the Idaho National Laboratory (INL), specializing in Cyber-Informed Engineering since September 2023. Previously, I held a position as a faculty member in the ICS Cybersecurity program at Idaho State University, where I was a Joint Appointee with the INL. My professional journey includes significant roles at the Naval Nuclear Laboratory (NNL), where I served as an Operational Technology (OT) Enterprise Architect, Systems Analyst, and a Controls Engineer. In these roles, I formulated the OT technical strategy and implemented a nation-wide OT infrastructure between the NNL's process systems. As a Control Engineer, I maintained a myriad of process and monitoring systems within power distribution, water and wastewater management, building automation, and radiological monitoring. I have a Bachelor of Science in Electrical Engineering from the University of Wyoming, and a Master of Science in Computer Science from the University of Idaho.

**Joshua Tannehill**

**Information Systems Security Officer | VP Louisiana Chapter, Knight Federal Solutions | InfraGard**

Knight Federal Solutions – Information Systems Security Officer
Support US Army at JRTC at Fort Polk to protect their classified network

Global Data Systems – Cybersecurity Sales Engineer
Support our sales teams as a cybersecurity subject matter expert in a sales analyst and sales engineering type of consultancy role.

Lumen Technologies – Senior Manager, InfoSec
People manager of a 9 person Trust & Safety team that supported Law Enforcement Support requests and kept the internet clean from cybercrime and abuse.

US Air Force and Air National Guard
Iraq war veteran and Protected the US Air Force from cyber-attacks and was the equivalent of the Chief Cybersecurity Compliance Officer for the Louisiana Air Force National Guard upon retirement in 2019.

**Lauren Nash**

**Warning Coordination Meteorologist, National Weather Service,**

Lauren Nash has been the Warning Coordination Meteorologist at NWS New Orleans/Baton Rouge since September 2020. Her main job is to interface and interact with our local partners, making sure their needs are met and our products are well understood. She also oversees community outreach, quality control, improvements of our products and overall ensuring we are a great partner in our community. Previously, she worked in Tallahassee, FL, Huntsville, AL, and New York City. She has a Bachelor's degree in Meteorology and a Master's Degree in Public Administration. In her free time, she enjoys relaxing with her two cats, scuba diving, traveling and enjoying all the city of New Orleans has to offer. She has an Undergraduate degree in Applied Meteorology with Minors in Aviation Operations and Airport Business from Embry-Riddle Aeronautical University. She has a Master's in Public Administration from Park University.


**Tommy Waller**

**President & CEO, Center for Security Policy**

Lt. Col. Tommy Waller, USMC Ret is the President and CEO of the nonprofit Center for Security Policy. Waller retired from the Marine Corps Reserves at the rank of Lieutenant Colonel after serving more than two decades on both active duty and in the reserves with deployments to Afghanistan, Iraq, Africa, and the Caribbean. His last military assignment was as the Commander of the Marine Corps Reserve's only Force Reconnaissance Company. While in the Corps, he graduated from the Marine Corps Command and Staff College and was cross assigned to serve as a key staff member of the U.S. Air Force's Electromagnetic Defense Task Force (EDTF). During his decade of civilian service to the Center for Security Policy he has led the nationwide "Secure the Grid Coalition," helping inspire policies to secure this most critical infrastructure at the federal, state, and local levels. Waller holds a BA in International Relations from Tulane University, New Orleans, LA and was the first recipient of the Captain Robert M. Secher Scholarship to the Wharton School of Business where he completed an executive education course on high stakes negotiations.

**Charles Burton,**
Technology Director, Calcasieu Parish Government

Charles Burton has led technology teams in Louisiana government for 20 years and is currently the Calcasieu Parish Technology Director. Data Center and communication modernization projects along with Cybersecurity programs have been some of his successful accomplishments with disaster recovery being one of the more challenging success stories. He holds a Masters in Cybersecurity and bachelor's in computer science. His certificates include ITIL, PMP, CGCIO, CISSP, CompTIA as well as Microsoft certificates.

Mr. Burton serves on several boards and committees at the State and Local level, he speaks at conferences and advises on the topics of Cybersecurity & Technology. Mr. Burton is involved in several community organizations where he resides in Lake Charles, LA with his wife and family.

**John Donlon**

Chairman, International Association Of CIP Professionals

John Donlon joined the police service in 1976 where he served in a wide variety of roles including; operational policing, major crime investigation, training and specialist operations. He was an accredited Gold Commander for Firearms, Public Order and Major Sporting Events. He was also a qualified Senior Investigating Officer.

In July 2005, as a Chief Officer, John was appointed to a National role within the world of Counter Terrorism and National Security, working with the Association of Chief Police Officers, Metropolitan Police (New Scotland Yard) and the UK Government. It was here that he provided the strategic policing lead on all matters within the Protect and Prepare portfolio of the UK Counter Terrorism Strategy, CONTEST.

Within his Protect remit he was accountable for the oversight of Special Branch and protective security policing at ports-encompassing all modes of transport, the National Counter Terrorism Security Office (NaCTSO) and the police contribution to protecting Crowded Places and the UK Critical National Infrastructure.

For Prepare, he had responsibility for the national police response to effectively manage a range of terrorist attacks, as outlined in the National Risk Assessment, building resilience, the national Counter Terrorism training portfolio and incorporating learning from CT incidents and exercises.


**Dr Ron Martin, CPP, CPOI**

**Professor Of Practice, Critical Infrastructure, Capitol Technology University**

Dr. Martin is a Professor of Practice at Capitol Technology University. His work at Capitol Technology University is in the following functional areas Critical Infrastructure, Industrial Control System Security, Identity, Credential, and Access Management. Ron has relationships with a diverse mix of businesses. He serves as a board of directors for many profit and non-profit organizations. Ron retired from the United States (U. S.) Army in 1999 and the U. S. Government in 2011. In between his Federal Service tours, he served five years as a civilian police officer in the Commonwealth of Virginia. During his Federal Service, he served with the U. S. Department of Commerce and Health and Human Services as the program director to develop and implement both department's Identity, Credentialing and Access Management (ICAM) Programs. Ron is a voting member of the United States Technical Advisory Group to the International Standards Organization (ISO), which works to develop and articulate the U.S. position by ensuring U.S stakeholders' involvement from the private and public sectors. Dr Martin serves as the North Louisiana Vice President of the InfraGard Louisiana Membership Alliance (ILMA). At ILMA he serves as the Critical Infrastructure Protection, Commercial Facilities Sector Chief. Ron holds a Ph.D. Technology, Capitol Technology University, a Master of Science in Management, Frostburg State University, Bachelor's degree in Police and Public Administration, George Mason University, and an AAS Degree in Police Science, Northern VA Community College.

**Joseph Threat**

**Chief Resilience Officer and Chief Administrative Officer, City of New Orleans**

Joseph Threat brings over four decades of distinguished expertise in crisis management, grant management, security training, executive municipal infrastructure operations/construction and emergency operations across both military and civilian sectors.

Beginning his career in the United States Marine Corps in 1968, Mr. Threat served multiple tours in Vietnam, accumulating over 26 years of service and retiring as a senior Warrant Officer. His military accolades include the Meritorious Service Medal, Navy Commendation medal with Combat "V" for Valor, and others recognizing his leadership and bravery.

Transitioning to civilian life, Mr. Threat assumed the role of Chief Executive Officer at Innovative Logistic Support Services (ILSS), where he spearheaded its growth into a multi- million-dollar business. Following this, he founded "Threat Defense," his consulting firm, providing strategic guidance until 2018. Notably, Mr. Threat served as Executive Director for FEMA's Louisiana Recovery Office, overseeing $37 billion in recovery funding post-Hurricanes Katrina, Rita, and other major disasters.

Currently serving an eight-year term as the Chief Resilience Officer and as the recently appointed Chief Administrative Officer for Infrastructure in the City of New Orleans. Mr. Threat plays a pivotal role in managing operations, emergency response, and capital projects. He has navigated numerous crises, including the Hard Rock Hotel collapse, Terrorist attacks, the COVID-19 pandemic, Super Bowl XIV and multiple hurricanes, demonstrating his steadfast leadership and commitment to public service.

**Josie Ross**

**Emergency Management Officer, City of Henderson Department of Emergency Management**

Josie Ross is the Emergency Management Officer for the City of Henderson Department of Emergency Management. Her work focuses on Continuity Planning, ICS training, exercises, hazardous materials and large scale special events. She is part of the planning team and serves as ESF 5 at the County MACC for the Superbowl, Formula 1 and New Year's Eve. She is the co-chair of the CAER group and serves on the LEPC and SERC. She has a Masters Degree in Emergency Management.


**Andrea Davis**

**President and CEO, The Resiliency Initiative, USA**

Andrea Davis is a recognized expert in the field of emergency management who has dedicated her career to bridging the silos between the public and private sectors to create a united approach when it comes to disaster risk reduction.

Ms. Davis has held leadership roles with NGOs (The American Red Cross, Save the Children US), the US Federal Government (FEMA, The Federal Reserve) and for Fortune 500 Companies (Walmart, Disney). With each role, Ms. Davis used her influence to lead global initiatives focused on the importance of making risk-informed determinations and engaging all members of the community in the decision-making process. Currently, Ms. Davis is the President and CEO of a Women Owned Small Business (WOSB), The Resiliency Initiative (TRI). Ms. Davis founded TRI out of a passion to serve the whole community before, during, and after an emergency.

Ms. Davis is a decorated leader. She was selected as the inaugural Emergency Manager of the Year by the International Association of Emergency Managers in 2018 and was inducted into the Women's Hall of Fame for Emergency Management in 2013.

**Michael Lambert**

**Emergency Preparedness/Homeland Security Planner, Houston-Galveston Area Council of Governments**

Michael Lambert is an Emergency Preparedness/Homeland Security Planner for the Houston-Galveston Area Council of Governments. Michael is an experienced emergency manager with nearly two decades working on issues related to the electric grid.

Michael has been a frequent panellist and speaker on the emergency management perspective of electric grid fragility, threats and resilience.

Among the organizations of which Michael is a member are the Secure the Grid Coalition, the Electric Infrastructure Security Council and the Texas Energy Working Group. He serves on the Texas Critical Infrastructure Protection Task Force and is an Infrastructure Liaison Officer with the State of Texas.

**Dr. Brenda Connor**

**Senior Technical Managing Director, TTU Critical Infrastructure Security Institute, USA**

Dr. Brenda Connor has a dual appointment at Texas Tech University as Professor of Practice in the Department of Electrical and Computer Engineering and as Senior Technical Managing Director for the Critical Infrastructure Security Institute (CISI). CISI's mission is to advance the protection, resilience, and security posture of our nation's critical infrastructure systems by developing cutting-edge solutions to emerging security challenges through interdisciplinary research, innovative education, and strategic partnerships. Dr Connor joined TTU in Jan 2025 after a 30-year career with Ericsson and is focused on applied research to accelerate the critical infrastructure operator's business case to deploy a private cellular network.

Her research areas include:
• Critical Infrastructure Security and Operational Efficiency via Private Cellular AI enabled Integrated Sensing and Communications (ISAC) and SCADA IO processing capability for national security with dual use relevance for DOD.
• NVIDIA based AI Model & Algorithms development and reuse.


**Ed Landgraf**

**Chairman, CAMO Pipeline Group and Director of Texas 811 Marine Safety and Operations**

Ed is the founder of CAMO "Coastal And Marine Operators" non-profit Pipeline industry group and serves as Chairman of the Board. Ed is also employed by Texas 811 as Director of Marine Safety and Operations. Ed is also the Pipeline Sector Chief of Louisiana Infraguard.

Ed has worked in the oil and gas industry for 33 years. A native of Oklahoma and graduate of Oklahoma State University, Ed's first assignments started in Texas, New Mexico, and Colorado. Ed then spent 26 years dedicated to Gulf Coast Region with special assignments in New Zealand and Australia. His roles included managing infrastructure protection, security, risks management, 811 education, marine safety processes, corporate sustainability, and many innovative initiatives. Ed is also an expert witness for marine pipeline accidents.

Ed has 17 years of volunteer service to the community as Vice- Chairman of Coastal Zone Management, Chamber of Commerce Board of Directors, member of the National Estuary Program's Management Committee, and Coastal Conservation Association Board of Directors.

Ed founded CAMO – "Coastal And Marine Operators" group in 2009. CAMO now has over 30 participating companies, NGO's and agencies, all working to enhance underwater infrastructure security, integrity, damage prevention, and public safety by designing and implementing new innovative solutions.

**Marco Ayala**

**President, Houston InfraGard Members Alliance**

Marco Ayala has 30 years of field experience where he designed, implemented, and maintained process instrumentation, automation systems, safety systems, and process control networks. In his role with large global manufacturing company, he is responsible for applications globally that are specific to plant site operations and corporate governance.

With around two decades focused specifically on industrial cybersecurity, he has led efforts to secure the oil and gas (all streams), maritime port, offshore facilities, and chemical sectors, supporting federal, local, and state entities for securing the private sector.

Marco is highly active in International Society of Automation and is a longtime member and newly elected into the Executive Board. He is a 22-year Senior Member and a certified cyber instructor for ISA (62443) with volunteering commitments and contributor to the AMSC Gulf of Mexico (GOM) cybersecurity committee in a sworn in role to the USCG as Chair of Threat Intelligence and Cybersecurity for the outer continental shelf (OCS).

InfraGard member since 2014, and currently serving as the President for the Houston Members Alliance.

**Full speaker lineup at www.ciprna-expo.com/speakers**


# DELEGATE REGISTRATION FORM

## EARLY BIRD SAVINGS

**Book your delegate place by 10th February 2026 and save with the Early Bird rate**

## REGISTRATION IS SIMPLE

1. Register online at www.ciprna-expo.com/register
2. Complete this form and email to: ciprna@torchmarketing.co.uk
3. Complete this form and mail to: CIPRNA 2025, Torch Marketing, 200 Ware Road, Hoddesdon, Herts EN11 9EY, UK.

## DELEGATE DETAILS

(Please print details clearly in English. One delegate per form, please photocopy for additional delegates.)

Title: _____ First Name: _____

Surname: _____

Job Title: _____

Company: _____

E-mail: _____

Address: _____

Street: _____

Town/City: _____

County/State: _____

Post/Zip Code: _____

Country: _____

Direct Tel: (+ ) _____

Mobile: (+ ) _____

Direct Fax: (+ ) _____

Signature : _____ Date: _____

*(I agree to the Terms and Conditions of Booking)*

## CONFERENCE FEES

**GOVERNMENT, MILITARY AND PUBLIC SECTOR/AGENCY**
**Individual Full Conference**
*(includes 3 day conference, conference proceedings, keynote, exhibition, networking reception, coffee breaks and 2 lunches)*

- ☐ Paid before 11th February 2026 ..... $195
- ☐ Paid on or after 11th February 2026 ..... $295

**OPERATORS/OWNERS OF INFRASTRUCTURE**
**Individual Full Conference**
*(includes 3 day conference, conference proceedings, keynote, exhibition, networking reception, coffee breaks and 2 lunches)*

- ☐ Paid before 11th February 2026 ..... $195
- ☐ Paid on or after 11th February 2026 ..... $295

**COMMERCIAL ORGANISATIONS**
**Individual Full Conference**
*(includes 3 day conference, conference proceedings, keynote, exhibition, networking reception, coffee breaks and lunch)*

- ☐ Paid before 11th February 2026 ..... $595
- ☐ Paid on or after 11th February 2026 ..... $895

**Exhibitor Full Conference**
*(includes 3 day conference, conference proceedings, keynote, exhibition, networking reception, coffee breaks and lunch)*

- ☐ Paid before 11th February 2026 ..... $295
- ☐ Paid on or after 11th February 2026 ..... $450

**Student Full Conference**
*(includes 3 day conference, conference proceedings, keynote, exhibition, networking reception, coffee breaks and lunch) - Student ID required*

- ☐ Paid before 11th February 2026 ..... $195
- ☐ Paid on or after 11th February 2026 ..... $195

- ☐ **Conference Proceedings only** ..... $495
- ☐ **EXHIBITION ONLY** (on-site registration $50) ..... $10

*(includes access to exhibition floor only)*

### Terms and Conditions of Booking

**Payment**: Payments must be made with the order. Entry to the conference will not be permitted unless payment has been made in full prior to 10th March 2026.
**Substitutions/Name Changes**: You can amend/change a delegate prior to the even start by notifying us in writing. Two or more delegates may not 'share' a place at an event. Please ensure separate bookings for each delegate. Torch Marketing Co. Ltd. reserve the right to refuse entry.
**Cancellation**: If you wish to cancel your attendance to the event and you are unable to send a substitute, then we will refund/credit 50% of the due fee less a $100 administration charge, providing that cancellation is made in writing and received before 11th February 2026. Regretfully cancellation after this time cannot be accepted. If we have to cancel the event for any reason, then we will make a full refund immediately, but disclaim any further liability.
**Alterations**: It may become necessary for us to make alterations to the content, speakers or timing of the event compared to the advertised programme.
**Data Protection**: Torch Marketing Co. Ltd. gathers personal data in accordance with the UK Data Protection Act 1998 and we may use this to contact you by telephone, fax, post or email to tell you about other products and services.
Please tick if you do not wish to be contacted in future by:

☐ Email ☐ Post ☐ Phone ☐ Fax

## PAYMENT DETAILS

(METHOD OF PAYMENT - 10.5% SALES TAX WILL BE ADDED TO FEES.)

☐ Wire Transfer (Wire information will be provided on invoice)

☐ Credit Card
*Invoice will be supplied for your records on receipt of the order/payment.*

Please fill in your credit card details below:
☐ Visa ☐ MasterCard

All credit card payments will be subject to standard credit card charges.

Card No: _____

Valid From ____ / ____ Expiry Date ____ / ____

CVV Number _____ (3 digit security on reverse of card)

Cardholder's Name: _____

Signature: _____ Date: _____

*I agree to the Terms and Conditions of Booking.*

**Complete this form and email to ciprna@torchmarketing.co.uk**