critical infrastructure PROTECTION AND RESILIENCE N. AMERICA

March 12th-14th, 2024

L'Auberge Hotel & Casino

LAKE CHARLES, 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 12th,2024

SPECIAL RATES FOR GOVERNMENT AND OWNER/OPERATORS
Register by February 12th
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

Platinum Sponsor:

TRUSTED COMPUTING GROUP

Silver Sponsors:

JCI | Security Products

ASSA ABLOY

HID VITAL INTEGRATORS

Leading the debate for securing America's critical infrastructure

Supporting Organisations:

INFRAGARD LOUISIANA · IACI · ISIO · ASIS UK · SEMI

Media Partner:

critical infrastructure PROTECTION AND RESILIENCE NEWS

A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Welcome to the 6th 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 security, national economic security, national public health or safety.

Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure. This directive supersedes Homeland Security Presidential Directive 7.

We must be prepared!

The Nation's critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure – including assets, networks, and systems – that are vital to public confidence and the Nation's safety, prosperity, and well-being.

Critical infrastructure must be secure and able to withstand and rapidly recover from all hazards. Achieving this will require integration with the national preparedness system across prevention, protection, mitigation, response, and recovery.

This directive establishes national policy on critical infrastructure security and resilience. This endeavor is a shared responsibility among the Federal, state, local, tribal, and territorial (SLTT) entities, and public and private owners and operators of critical infrastructure (herein referred to as "critical infrastructure owners and operators"). This directive also refines and clarifies the critical infrastructure-related functions, roles, and responsibilities across the Federal Government, as well as enhances overall coordination and collaboration. The Federal Government also has a responsibility to strengthen the security and resilience of its own critical infrastructure, for the continuity of national essential functions, and to organize itself to partner effectively with and add value to the security and resilience efforts of critical infrastructure owners and operators.

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

The conference will look at developing on the theme of previous events in helping to create better understanding of the issues and the threats, to help facilitate the work to develop frameworks, good risk management, strategic planning and implementation.

Why the Need for Such a Discussion?

All Federal department and agency heads are responsible for the identification, prioritization, assessment, remediation, and security of their respective internal critical infrastructure that supports primary mission essential functions. Such infrastructure needs to be addressed in the plans and executed to the requirements of the National Continuity Policy.

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 demands.

This guide, correct at the time of printing, aims to provide you with the information you need to plan your attendance to this key conference, including the latest conference programme, speaker line up and schedule of events.

We have special rates for government and operators of critical national infrastructure, so please look fr these deals in this guide.

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

We look forward to welcoming you to Critical Infrastructure Protection & Resilience North America and the L'Auberge Hotel & Casino, Lake Charles, LA on March 12th-14th, 2024.

Follow us:

Critical Infrastructure Protection & Resilience Europe

A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

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 Lake Charles, Louisiana, for what will be 3 days of exciting and informative discussions on securing North America's critical infrastructure.

This is our 5th annual conference here in the United States and follows on from our very successful European event which took place in Prague in October 2023. This year we are delighted to have the support of a number of organisations, which include InfraGard Louisiana, the International Association of CIP Professionals, The International Emergency Management Society and International Association of Certified ISAOs.

There is an exciting line up of topics and 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 governments 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 infrastructure sectors.

The last few years has seen the world immersed in a period with significant challenges and a great deal of uncertainty. The war between Russia and Ukraine continues unabated and has recently been somewhat overshadowed, in the media at least, by the conflict between Israel and Hamas. The loss of life and the utter devastation that has been caused is deeply concerning as is the obvious impact that both wars have on the position of Global Peace and Security.

The protection and resilience of our infrastructure and information systems against malicious attacks and natural disasters are crucial issues for all society. We have seen record temperatures being recorded throughout 2023 and through this we have seen devastating wildfires, flooding and earthquakes and not a day goes by without there being some reference to the potential of a cyber-attack significantly affecting the very core of our critical infrastructure.

There is, therefore, a continual need to review, develop and update policies, practices, procedures and technologies to meet those growing and changing demands.

In seeking to address 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 Lake Charles.

John Donlon QPM FSyl
Conference Chair

A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

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:

- 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 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 Lake Charles, LA 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."

A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Exhibition Opening Hours		On-Site Registration Hours	
Tuesday March 12th	1.00pm to 7.30pm	Tuesday March 12th	8.00am to 6.00pm
Wednesday March 13th	9.30am to 5.30pm	Wednesday March 13th	8.30am to 5.00pm
Thursday March 14th	9.30am to 4.30pm	Thursday March 14th	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 federal government, emergency management agencies, emergency response and law enforcement or inter-governmental agencies, DHS, CISA, FEMA, TSA, DISA, GAO, NSA, NCTC, 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 infratructure 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 12th, 2024

Register yourself and your colleagues as conference delegates by February 12th, 2024 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 LA
- The International Emergency Management Society (TIEMS)
- National Security & Resilience Consortium (NS&RC)
- International Association of CIP Professionals (IACIPP)
- International Security Industry Organization (ISIO)
- International Association of Certified ISAOs (IACI)

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

A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Schedule of Events

Tuesday March 12th, 2024

8.30am - 12.30pm - Site Visit (for delegates registered for the site visit)

1:00pm - Exhibition Opens

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

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

4.00pm-5:30pm - Session 1: CI Interdependencies and Cascading Effects in Community Situational Awareness

5:30pm - Networking Reception in Exhibition Hall

Wednesday March 13th, 2024

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: Communications Sector Symposium

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

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

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

4:15pm - 5:30pm - Session 5a: Critical Industries Sector Symposium

Track Two

9:00am-10:30am - Session 2b: Cybersecurity Regulations, Best Practice and Minimum Standards

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

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

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

2:00pm-3:30pm - Session 4b: Transport Sector Symposium

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

4:15pm - 5:30pm - Session 5b: Information Technology (CIIP) / Cybersecurity Symposium

Thursday March 14th, 2024

9:00am-10:30am - Session 6a: Modeling and Methodology Around Incident Mitigation & Emergency Management

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

11:15am - 12:30pm - Session 7a: Insider Threat

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

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

11:15am - 12:30pm - Session 7b: Strategic Resilience Planning

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 - Expo Close

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

A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Site Visit

CITGO Lake Charles Refinery

Tuesday 12th March – 8.30am-12.30pm

A great opportunity to see how a key CI delivers protection, security and resiliency plans to their operations.

Book your place online at www.ciprna-expo.com/register

We are delighted to offer, in cooperation with **CITGO and CISA Region VI**, the opportunity to visit the CITGO Lake Charles refinery, and discover how the company develops and implements its resiliency planning to ensure security of operations and supplies.

With limited spaces available, this Site Visit is offered an a first come first served basis – please book your place on the site visit today to secure your place on this interesting and exciting site visit.

Lake Charles Refinery

The Lake Charles Refinery is the seventh-largest refining facility in the United States and has gained a reputation as one of the safest facilities in the industry. As the largest of the three CITGO refineries, the Lake Charles Refinery consists of a modern, deep-conversion facility with a crude oil refining capacity of 463,000 barrels per day (bpd).

About CITGO

CITGO Petroleum makes the products that fuel everyday life. They company refines, transports and markets motor fuels, lubricants, petrochemicals, and other industrial products.

When natural disasters strike the communities where we live and work, CITGO lends a helping hand not only in the immediate aftermath but also long term. From Hurricane Harvey to the more recent Winter Storm Uri, we helped our neighbors in need by providing:

- Short-term immediate assistance to support local partners working on recovery efforts

- Long-term assistance to repair homes, rebuild communities and get them back to normal

- Equipment for first responders and community organizations designed to prepare for and accelerate recovery.

A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Exhibitor Showcasing in the Expo:

The CIPRNA Expo showcases some of the latest and leading technologies and solutions for protection and securing critical infrastructure from today's cyber-physical threats.

Pre-Register for your Expo Only Pass at just $10
www.ciprna-expo.com/onlinereg
($50 on-site registration)
*Includes coffee

A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Tuesday March 12th

Conference Programme

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

Chair: John Donlon QPM, FSI
International adviser on security intelligence

Representative for Congressman Clay Higgins

Steve Harris, Deputy Executive Assistant Director for Infrastructure Security, Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA)

Senior Representative, Governors Office of Homeland Security & Emergency Preparedness

Mayor Nic Hunter, Mayor of lake Charles

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

4:00pm-5:30pm - Session 1: CI Interdependencies and Cascading Effects in Community Situational Awareness

It is the interoperability between independent critical national infrastructures that is the catalyst for multiple failures in the so called cascade effect. As more infrastructure becomes increasingly interdependent, how do we identify the weaknesses to enhance resilience across industries to prevent and/or mitigate the effects of a natural disaster or man-made attack? How should the CI community build situational awareness to mitigate the cascading effect across infrastructures.

Chair: John Donlon QPM, FSI

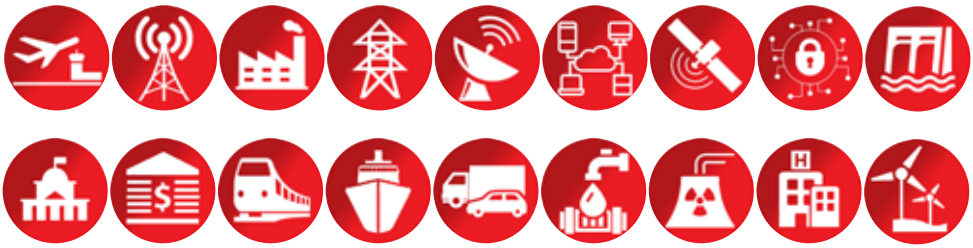
Adam Stahl, Chief of Staff Corporate Security, AVANGRID

Anna Ballance, Sr. Advisor, Industry Policy Coordination, E-ISAC
Cameron Dicker, Director of Global Business Resilience, FS-ISAC
Chris Anderson, Co-Chair, Comm-ISAC

Critical Infrastructure Dependency Analysis - National Laboratory Research and Development Advancements - Dr. Ryan Hruska, Chief Scientist - Infrastructure Dependency Analysis, Idaho National Laboratory; Dr. Joshua Bergerson, Principal Infrastructure Analyst, Argonne National Laboratory; Tim McPherson, Research Scientist, Pacific Northwest National Laboratory, USA

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

**invited*



A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Wednesday March 13th

Track One

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

The ever changing nature of threats, whether natural, through climate change, or man-made through terrorism activities and insider threats, and coupled together with the latest challenges with cyber attacks from many directions, creates the need to continually review and update policies, practices and technologies to meet these growing demands. But what are those emerging threats, both physical and cyber, and how can we identify, monitor and manage their levels of potential damage?

Associate Special Agent in Charge, FBI

Drones as a Threat Vector to Critical Infrastructure - Michael Hill, Program Specialist, Cybersecurity and Infrastructure Security Agency

Doug Cramer, Warning Coordination Meteorologist, National Weather Service

Cyber Threats to the US Emergency Services Sector - Richard Tenney, Senior Advisor, Cyber, Cybersecurity and Infrastructure Security Agency (CISA)

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

11:15am-12:30pm - Session 3a: 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 vital for businesses, government and all sectors of CI.

Revolutionizing 5G Operations and Security with Automation - Dr. Srinivas Bhattiprolu, Global Head of Advanced Consulting Services, Nokia

Joshua Tannehill, Technical Sales Consultant, Global Data Systems & Vice President of Communications Sector, Infragard LA

Chris Anderson, Co-Chair, Comm-ISAC & Principal Advisor, National Security and Emergency Preparedness at Lumen Technologies

Social Network Analysis - Michael Aspland, Executive Director, Institute for Homeland Security, Sam Houston State University

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

Track Two

9:00am-10:30am - Session 2b: Cybersecurity Regulations, Best Practice and Minimum Standards

As the threat of cyber-attacks by state actors grows ever higher and attacks by criminals and malicious rogue players continues unabated the need to put in place robust legislation and standards and best practice becomes all the more urgent. What is the latest on the Cyber Incident Reporting for Critical Infrastructure Act and developing regulations around AI in cybersecurity?

CIRCIA – Cyber Incident Reporting for Critical Infrastructure Act - Senior Representative, Directorate for Cybersecurity, CISA*

Conducting State-wide Critical Infrastructure Cyber Risk Assessments: The Florida Experience - Emilio Salabarria, Senior Program Manager for Cybersecurity, The Florida Center for Cybersecurity: Cyber Florida & Tim Klett, Strategic Technology Integration Strategist, Idaho National Laboratory

Deborah Kobza, President, International Association of Certified ISAOs

Strategic Governance of Cybersecurity and AI Risk - Keyaan Williams, Managing Director, Cyber Leadership and Strategy Solutions, CLASS LLC

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

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

Pipelines and associated land-based infrastructure along the chain are vulnerable to technical or human failures, natural disasters, cyber-attacks, terrorist threats and other emerging risks, as well as from geopolitical disputes. Disruptions along single transport routes can threaten the uninterrupted supply across the broader network. Protecting oil and gas assets and improving resilience while meeting operational and regulatory requirements is of high priority worldwide, particularly in times of heightened tension.

Melvin Carraway, Region 4 Security Director, Transport Security Administration

Energy Pipeline Safety and Security - Ed Landgraf, Chairman, Coastal And Marine Operators

Drones and Threats to Pipelines - George Rey, President, COTS Technology & Vice Chair, Pelican Chapter AUVSI, USA

Ben Dierker, Executive Director, Alliance for Innovation and Infrastructure, Institute for Homeland Security

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

A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Wednesday March 13th

Track One

2:00pm-3:30pm - Session 4a: Power & Energy Sector (Grid Resilience) 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 vital for businesses, government and all sectors of CI.

Chair: Tommy Waller, President and CEO, Center for Security Policy

The Electric Grid - Nathan Landry, Intel Support Coordinator, Entergy Services

Bob Janusaitis, President, InfraGard San Antonio Members Alliance

Euclid Talley, Branch Manager, Critical Infrastructure Protection, Governors Office of Homeland Security & Emergency Preparedness

Motivating action via a climate resilience maturity model for critical infrastructure owners and operators - Andrew A Bochman, Senior Grid Strategist-Defender, DOE / Idaho National Lab

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

4:15pm-5:30pm - Session 5a: Critical Industries Sector Symposium

Critical Industries security practices are frequently integrated across industry (especially with increasingly converging physical and cyber technologies), they can be organized into four major categories: physical, cyber, personnel, and supply chain. Combining manufacturing, or other key processes, with the need for resilient logistical operations, including in IT/OT and SCADA systems, in order to ensure reliable and timely delivery is key to any thriving economy.

Securing Your Chemicals: Voluntary Tools and Services to Assess and Mitigate Risk - Bryan McDonald, Acting ChemLock Program Manager at the Cybersecurity and Infrastructure Security Agency

Dan Frazen, CO-CEM, Agriculture Emergency Coordinator (All-Hazards), Colorado Dept of Agriculture

Cyber-physical convergence: How cyber incidents can impact the physical world - Cameron Dicker, Director of Global Business Resilience, FS-ISAC

Untrusted Execution: Attacking the Critical National Infrastructure Software Supply Chain - Francesco Beltramini, Security Engineering Manager, ControlPlane

Track Two

2:00pm-3:30pm - Session 4b: 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.

Ronald Pavlik, Deputy Assistant Administrator, Surface Operations, TSA*

Senior Special Agent Jack Bartlett, Union Pacific Railroad Police Department

What can we learn from Behaviour - Sarah Jane Prew, Senior Security Advisor, Arup

By Land, Air and Sea: Getting Stakeholder Buy-In to Protect Our Nation's Supply Chain - Theresa Jones, CSA, CMMC-RP, Owner and Principal Consultant, Evalv IQ

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

4:15pm-5:30pm - Session 5b: Information Technology (CIIP) / Cybersecurity Symposium

Securing the digital infrastructure. Information technology is responsible for such a large portion of our workforce, business operations and access to information and data, Critical Information Infrastructure Protection (CIIP) through cybersecurity and network security, is vital to protect information assets. Recent ransomware attacks and other threats, such as Malware, Stuxnet, etc and the continued cyber threats and intrusions, means we have to be more vigilant to protect our information assets. How do we better secure our data, can AI or DevSecOps play a role in CI cyber protection and threat detection?

The implementation of Zero Trust in Critical Infrastructure - Ron Martin, Professor of Practice, Capitol Technology University

Head of Sector, AI-ISAC*

Beyond Physical Security: Using Data to Improve Operation - Greg Kemper, Regional Director, Enterprise Solutions, Genetec

Roman Gonzales, Sr Systems Engineer, Veeam Software, USA

The Argument for a Converged Cybersecurity Strategy - Darrin Swan, Co-Founder and VP Sales, Todyl

A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Thursday March 14th

Track One

9:00am-10:30am - Session 6a: Modeling and Methodology Around Incident Mitigation & Emergency Management

Predicting how threats can impact business continuity of critical assets can be of major benefit for planning resiliency or emergency response. This affects both financial and resource planning. So what are the latest roles and assessments in modeling and methodology? What role can machine learning and AI play in building more accurate predictions and what measures can be put in place to mitigate risk?

Best Practices in Climate Resiliency – How to Mitigate Your Industry's Impact - Sunny Wescott, Lead Meteorologist, Cybersecurity and Infrastructure Security Agency

Modeling Critical Infrastructure Reliability for Military Bases - Alexander Ankney, Cadet First Class, United States Air Force Academy

Protecting mission-critical networks from quantum attacks - Chris Janson, Sr. Industry Analyst, Nokia

FREE HAZMAT/CBRNE Incident Support - The Interagency Modeling and Atmospheric Assessment Center - Sloan Grissom, Counterterrorism Practice Lead/Outreach Coordinator, Interagency Modeling and Atmospheric Assessment Center

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

11:15am-12:30pm - Session 7a: Insider Threat

An insider threat is a perceived danger to your company that originates from individuals who work there, such as current or former employees, contractors, or business partners, who have inside knowledge of the company's security procedures, data, and computer systems. The main objectives of malevolent insider threats are espionage, fraud, intellectual property theft, and sabotage, for monetary, private, or malicious purposes, they wilfully misuse their priviledged access to steal information or damage systems. Here we take a deeper dive into the range of threats and how to mitigate and counter these.

Sarah-Jane Prew, Senior Security Advisor, Arup UK

Jim Henderson, CEO, Insider Threat Defense Group

Achieving Critical Infrastructure Sector-Focused Cybersecurity Workforce - Ralph Ley, Director, Workforce Development Program Office, Idaho National Laboratory

TBC

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, underwater, or airspace awareness technologies, access controls, and space based or cyber technology, 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.

Cyber Resilience - Senior Representative, Trusted Computing Group

Strengthening Security through Integration: Unleashing the Power of Combined Protection - Joe Morgan, Business Development Manager, Critical Infrastructure, Axis Communications

Safeguarding Critical Infrastructure in the Age of Drone Threats - Dennis Ziemba, VP of Sales and Operations, AeroDefense

The Unseen Threat - The Underwater Detection Problem - Simon Goldworthy, Wavefront Systems

Securing Critical Infrastructure using Radar Technology - Caleb Goldberg, Regional Sales Manager, JCI Security Products

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

11:15am-12:30pm - Session 7b: Strategic Resilience Planning

Being prepared for the changing threat environment can benefit greatly in mitigating its impact on infrastructure and the broader community, ensuring resilience, safety and security. How to we develop and plan the best resilience strategies within our CI community? Through discpline in information sharing and making infrastructure preparedness personal, we can help to build resilience into our infrastructures that benefit the whole community.

Improvised Explosive Devices and Critical Infrastructure Protection - Douglas DeLancey, Branch Chief Bombing Prevention, Cybersecurity and Infrastructure Security Agency

National Infrastructure Preparedness Realities and the Resilience Imperative - Jeff Gaynor, President, American Resilience

Storm-DEPART (Damage Estimate Prediction and Restoration Tool) - Ollie Gagnon, Chief Homeland Security Advisor, Idaho National Laboratory

IAM drivers in Critical Infrastructure Security - Charles Burton, Technology Director, Calcasieu Parish Government

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

A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Thursday March 14th

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

It is well established that information sharing and collaboration is essential for developing effective risk, resilience and emergency management planning. Information and Knowledge is key to make the right decisions to better plan to protect your assets. How do we break down the barriers to information sharing? How do we continue to build trust between government, operator/owners and the communities to enhance the PPPs impact on CI protection and resilience?

Moderator: John Donlon QPM FSI

Busting Info-Sharing Myths—engaging with CISA - Terrence Check, Senior Legal Council, CISA

CISA Introduction & Engagements with Industry and SLTT - Rola Hariri, Defense Industrial Base Liaison, Cybersecurity and Infrastructure Security Agency (CISA)

Lester Millet, President, Infragard Louisiana & Safety Risk Agency Manager, Port of South Louisiana

Protecting Critical Electric Infrastructure With a Community Cyber Force - Alex Brickner, Director of Small Business, Innovation, and Research Programs, University of Massachusetts Lowell Applied Research Corporation

Director, Homeland Security and Justice, GAO*

Senior Representative, FEMA*

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

Networking Reception

Tuesday March 12th
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.

A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Highlighted Speakers

Dr. David Mussington
Executive Assistant Director for Infrastructure Security, Cybersecurity and Infrastructure Security Agency (CISA)

Dr. David Mussington currently serves as the Executive Assistant Director for Infrastructure Security at the Cybersecurity and Infrastructure Security Agency (CISA). Since February 2021, he continues to lead CISA's efforts to secure the nation's critical infrastructure in coordination with government and the private sector. Key areas of focus include vulnerability and risk assessments; securing public gatherings; developing and conducting training and exercises; and securing high-risk chemical facilities.

Dr. Mussington has academic as well as private and public sector experience.

Immediately prior to joining CISA, Dr. Mussington was Professor of the Practice and Director for the Center for Public Policy and Private Enterprise at the University of Maryland School of Public Policy. His research and teaching activities focused on integrated cyber physical system risk management, election cybersecurity, and critical infrastructure security risk management. He is published in academic and professional journals, including published handbooks by the University of Oxford in the U.K., working papers co-written with partners at the U.S. Naval War College, and peer reviewed articles in the Institute of Electrical and Electronics Engineers outlets about metrics and risk frameworks for cyber defense. Most recently, he conducted projects on election cybersecurity, social media information security issues, and the security of Internet and Communications Technology supply chains.

Douglas Delancy
Branch Chief, Counter IED Strategy, Integration & Comms, Office For Bombing Prevention, CISA

Mr. Doug DeLancey currently serves as the Department of Homeland Security's Counter-Improvised Explosive Device (C-IED) Strategy, Integration and Communications Branch Chief in the Office for Bombing Prevention (OBP). Supporting the Office since January 2014, he has led the first national capabilities-based assessment to determine the capabilities to counter the threat of terrorist bombings. Doug is a former Army Colonel graduate from the U.S. Military Academy at West Point with a B.S. degree. He spent many deployments finding and attacking the networks responsible for employing improvised explosive devices.

Doug has a Master's Degree from the U.S. Army Command and General Staff College and the Central Michigan University, and has completed the Homeland Security Course at the Harvard Kennedy School of Executive Education in Cambridge, MA. He is a CPP and PMP.

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.

A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

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. Srinivas Bhattiprolu
Global Head of Advanced Consulting Services, Cloud and Network Services, Nokia, USA

As Nokia Cloud and Network Services' Global Head of Advanced Consulting Services and Presales head, Srinivas Bhattiprolu is primarily responsible for driving the Cloud and Network services portfolio business along with business consulting business for the company.

A result-oriented IT professional with over 22 years of techno-managerial experience, Srinivas has cultivated a strong understanding of the security domain, specializing in IoT Consulting and IoT Security, building solution blueprints and the corresponding use cases for communication service providers. He also possesses knowledge and working experience in various domains such as telecommunications, banking, financial services, and industrial process control.

Srinivas's professional accreditations include recognition as a Certified Information Security Manager (CISM) from ISACA (an international association focused on IT governance) and Certified Cloud Security Professional (CCSP) from (ISC)2.

Based in California, Srinivas holds a Bachelor of Technology in Instrumentation from the Andhra University College of Engineering in India. He also holds a PGDM in Finance and IS from the Xavier Institute of Management in India, in addition to a CGBL in General Management from U21 Global and a Certification in Organization Sustainability from the University of Cambridge. He also holds certifications from the Massachusetts Institute of Technology on Machine Learning and Blockchain. Srinivas Recently completed a leadership course from Said Business School, Oxford University. Srinivas has a professional Doctorate from Edinburgh Napier University where he focused his research topic on Organizational Sustainability.

Nathan Landry,
Intel Support Coordinator, Entergy Corporation, USA

Nathan Landry is currently an Intel Support Coordinator within the Security and Intelligence Support Team at Entergy Corporation. Entergy is one of the largest investor-owned utility companies located in the United States serving the Texas, Louisiana, Arkansas, and Mississippi. In this capacity, he focuses on collecting, analysing, and disseminating physical and cyber threat intelligence. Previously, he worked for the United States Secret Service as an investigative assistant in Baton Rouge, Louisiana. He then worked for the Louisiana State Police Fusion Center as an intelligence analyst on the strategic team focusing on critical infrastructure protection. Mr. Landry graduated from Louisiana State University in 2019 majoring in Political Science. He plans on graduating from Tulane University with a Master of Professional Studies in Homeland Security concentrating in Cybersecurity. Mr. Landry is an advocate for strengthening public-private sector relationships to foster better threat intelligence and information sharing.

A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Jim Henderson
CEO, Insider Threat Defense Group, Inc.,, Founder / Chairman, National Insider Threat Special Interest Group

Mr. Jim Henderson is the CEO of the Insider Threat Defense Group, Inc., Founder / Chairman Of The National Insider Threat Special Interest Group and U.S. Insider Risk Management Center Of Excellence.

Mr. Henderson has 20+ years of experience protecting sensitive and classified information up to the Top Secret SCI Level, with hands-on experience in the development, implementation and management of; Insider Threat Programs, Cyber Security – Information Systems Security Programs for U.S. Government Agencies, Department of Defense, Intelligence Community Agencies, Defense Contractors and State Governments.

Mr. Henderson's has an extensive background in many different IT – Network Security and other security related disciplines: Physical Security, Data Loss Prevention, Information Assurance, Certification & Accreditation Of Information Systems / Networks, Security Training & Awareness, Security Policies & Procedures Development, Insider Threat Investigations, Digital / Computer Forensics Investigations and Technical Surveillance Countermeasure Inspections.

Brian Harrell
Vice President and Chief Security Officer (CSO), Avangrid, USA

Brian currently serves as the Vice President and Chief Security Officer (CSO) at Avangrid, an energy company with assets and operations in 24 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).

Prior to his time at DHS, he spent considerable time at Duke Energy and the North American Elecric Reliability Corporation (NERC) where he worked to secure critical assets, employees, and information from attack and reputational damage.

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.

Ollie Gagnon III, CISSP, CPP, PSP
Strategic Advisor, Critical Infrastructure Security and Resilience, Idaho National Laboratory, USA

Ollie Gagnon is the Strategic Advisor, Critical Infrastructure Security and Resilience in the National & Homeland Security (N&HS) directorate at Idaho National Laboratory (INL). He serves as the primary representative and lead for U.S. Department of Homeland Security (DHS) efforts. N&HS supports the U.S. DHS operational and support components, and other federal agencies by providing unique capabilities to complex homeland security challenges. The DHS portfolio includes control systems security, infrastructure analysis and technology development, workforce development, and life-line infrastructure resilience. Mr. Gagnon also serves on the INL Resilience Optimization Center (IROC) Strategic Advisory Group.

A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Jeff Gaynor
President
American Resilience

"Status quo you know, is Latin for the mess we are in"
President Ronald Reagan

A Retired US Army Colonel, Jeff Gaynor brings six decades of highly decorated military and Defense Intelligence Senior Executive Service and since his retirement from Federal Service, Private Sector Critical Infrastructure (CI) and National Preparedness expertise to the most fundamental and urgent of National Preparedness imperatives. Specifically, ensuring the "all condition" operational resilience of America's CI. To that end, leveraging his experience as President Reagan's and George H.W. Bush's Communications Security Officer, as the Defense Department's Y2K Operations Officer and with President Reagan's quote in mind, nine months before the failure of a "protected" New Orleans Levee System, Jeff created and directed the Homeland Security Advisory Council's Critical Infrastructure Task Force (CITF). The CITF reviewed and questioned the efficacy of the CI status quo and in its January 2006 report, recommended that Critical Infrastructure Resilience be made ". . . the top-level strategic objective – the desired outcome to drive national policy and planning." 18 years later, Jeff continues to spearhead continuous and objectively measurable change in the CI status quo through advocacy for and implementation of operationally proven, nationally comprehensive and compatible, resilience-based CI, business and community preparedness mindsets, metrics, methodologies and technologies.

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.

Emilio Salabarria
Senior Program Manager for Cybersecurity, The Florida Center for Cybersecurity: Cyber Florida

Emilio is a native of Tampa, Florida. In July 2022, he joined Cyber Florida and is responsible for providing advanced, expert knowledge and subject matter expertise in a specific subject area that contributes to the mission(s) and initiative(s) of The Florida Center for Cybersecurity (aka Cyber Florida) at The University of South Florida (USF).

Emilio worked for the Tampa Electric Company (TECO) as the Emergency Management and Business Continuity Director, The Depository Trust and Clearing Corporation (DTCC) as the Global Life Safety Manager, the Tampa Port Authority (TPA) as the Director of Safety and Training, and Tampa Fire Rescue (TFR) where he advanced up the ranks to Division Fire Chief of Special Operations, supervising the TFR Specialty Teams. He participated as part of the TFR planning team for many Gasparilla Parades, the 2012 Republican National Convention (RNC), and Super Bowl 43.

A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

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.

Chris Janson
Sr. Market advisor, Nokia, USA

Chris Janson is a market advisor in Nokia's Network Infrastructure group. He follows trends in optical networking and security technologies and its application to enterprise and other network operators. He has long contributed to the communications equipment and semiconductor fields through engineering and marketing roles. Chris enjoys giving back to the community through teaching engineering courses and serving on volunteer boards. In between that, he can be found running, riding bikes or windsurfing on Cape Cod or Maui.

Rola Hariri
Defense Industrial Base Sector Liaison, Cybersecurity and Infrastructure Security Agency (CISA)

As CISA's Defense Industrial Base Sector Liaison, Ms. Hariri is the nexus for CISA's Defense Industrial Base (DIB) Sector efforts. She partners with the Department of Defense (DoD), the DIB Sector Risk Management Agency, as well as private and public stakeholders in the DIB Sector. In addition to supporting DIB efforts across CISA, Ms. Hariri, as CISA's representative on the DIB Government Coordinating Council, works with DoD and other government partners, as well as the DIB Sector Coordinating Council to address sector priorities and increase the resilience of our nation's critical defense infrastructure.

Prior to joining CISA, Ms. Hariri supported DoD's Office of the Under Secretary of Defense for Research and Engineering (OUSD/R&E) where she advised and coordinated on economic security matters as it relates to implementing technology promotion and protection programs for DoD's fourteen Critical Technology Areas (CTAs). Ms. Hariri's previous work includes implementing Department of State (DOS), Political-Military Bureau's global defense trade outreach strategy, where she also coordinated commercial defense trade plans and risk analysis for U.S. defense trade policy for the Middle East region. Additionally, Rola served at DOS' International Security & Nonproliferation Bureau (ISN) where she developed and maintained industry and foreign governments' partnerships for the Office of Export Control Cooperation with several international organizations including United Nations Office on Drugs and Crime (UNODC) and World Customs Organization (WCO). Before joining DOS, Rola started her career in the private sector and held numerous leadership positions that focused on implementing project management efficiencies and delivered successful strategies for administering a billion-dollar portfolio.

A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Budge Currier
Assistant Director Public Safety Communications, California Office of Emergency Services (Cal OES)

Since 2011 Budge has served with the California Office of Emergency Services (Cal OES). In his current role, Budge is responsible for the statewide public safety radio systems and microwave network that supports state agencies, the 9-1-1 system that supports 438 Public Safety Answering Points with over 27 million 9-1-1 calls per year, the 9-8-8 system, and the Emergency Communications Division. Budge also serves as the California Statewide Interoperability Coordinator (SWIC).

Budge has over 30 years of communication's experience and holds a Bachelor of Science degree in Computer Science from University of Michigan and a Masters Degree in Electrical Engineering from the Naval Postgraduate School in Monterey, CA. Budge is a member of NENA, APCO, and NCSWIC. Budge also serves as the Past President of the National Association of State 9-1-1 Administrators (NASNA).

Keyaan Williams
Founder & Managing Director
CLASS-LLC

Keyaan J. Williams is the Founder and Managing Director of CLASS-LLC, a professional services firm that specializes in corporate governance, enterprise risk, and cybersecurity program management for global customers. Prior to CLASS-LLC, he managed large security programs at the CDC. A founding member of the Private Directors Association Atlanta Chapter, he currently serves as the chair of the risk committee for a global non-profit and as a strategic advisor for other start-up and early-stage organizations. In addition to public speaking, his knowledge is documented in numerous books and publications such as the Certified CISO Body of Knowledge, The Language of Cybersecurity, Using Security Metrics to Drive Action, CISO Magazine, the ISSA Journal, and the Crisis Response Journal.

Terence Check
Senior Counsel for International Law and Infrastructure Security, CISA

Terence Check is Senior Counsel for International Law and Infrastructure Security in the U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) Office of Chief Counsel. In this role, Terence advises on operational law matters in support of CISA's critical infrastructure security mission, particularly on information-sharing and data protection, school safety, international relations, and strategic policy issues for the Infrastructure Security Division and CISA Office of International Affairs. Terence advises on constitutional and national security law issues while also managing CISA's repository of legal, regulatory, and policy authorities.

Prior to joining CISA, Terence served as an Attorney-Advisor in the DHS Office of the General Counsel's Operations and Enforcement Law Division. Terence advised DHS offices and components on matters involving screening/vetting, biometrics (including facial recognition and DNA), data privacy, and information-sharing issues. In this role, Terence served as a lead negotiator on Department-wide info-sharing and border security agreements across the Americas and Europe, finalizing complex technical agreements with several countries and participating in dozens of negotiations with senior staff and political leaders from more than 13 different nations. Terence also expanded DHS's biometric support to federal criminal prosecutions, resulting in scores of convictions for crimes ranging from naturalization fraud to drug smuggling.

A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Sunny Wescott
Lead Meteorologist, CISA

Sunny Wescott is a Lead Meteorologist specializing in national extreme weather hazards and climatological studies for impacts to public and private sector key resources. Her previous roles working with emergency response operations for Telecommunications and Critical Infrastructure integrated her background with mission support forecasting from her previous years in the US Air Force.

Ms. Wescott trained on continental and oceanic weather as the Top Forecaster for her support region and is considered a subject matter expert for multiple climatological events such as drought, subsidence, wildfires, tropical cyclones, and winter storms. Ms. Wescott graduated top of her class for her degrees in Homeland Security Management, Public Safety Administration, and Atmospheric Sciences. Her current role as CISA's Extreme Weather Outreach for the Infrastructure Security Division Collaboration Cell enables her to provide focused climate reports for regions and critical infrastructure operators.

Kimberly Heyne
ChemLock Program Manager, Cybersecurity and Infrastructure Security Agency (CISA)

Kimberly Heyne is the ChemLock Program Manager at the Cybersecurity and Infrastructure Security Agency within the Department of Homeland Security. In this capacity, she oversees the operations of the voluntary chemical security ChemLock program and manages the development of the services and tools it offers.

Previously, Ms. Heyne worked for the Defense Threat Reduction Agency as an International Program Manager, leading projects aimed at preventing the proliferation of weapons of mass destruction. Prior to starting her federal career, Ms. Heyne worked at the national headquarters of the American Red Cross. She holds a master's degree in International Affairs from the George Washington University's Elliott School of International Affairs.

Richard Tenney
Senior Advisor, Cybersecurity, Cybersecurity and Infrastructure Security Agency (CISA)

Richard Tenney serves as Senior Advisor for Public Safety Cybersecurity to the Executive Assistant Director of the Cybersecurity and Infrastructure Security Agency's Emergency Communications Division located in the United States of America. Since 2009, he has managed technical assistance and strategic planning for emergency communications for 56 states and territories. In collaboration with other CISA elements, he has led technical assistance efforts to support awareness and education of Public Safety Answering Points (PSAPs) and 9-1-1 functions about cyber threats to their operations, especially ransomware. He has presented at numerous national conferences including IWCE and APCO on cybersecurity and public safety communications. Prior to joining DHS, Tenney was an executive for IT and telecommunications consulting in Northern Virginia supporting clients like the FBI. He also served in the USAF as a special agent/counterintelligence officer. He holds undergraduate and graduate degrees from Georgetown University, University of Maryland, and Troy University including a BS in management information systems and programming. He is an ISACA Certified Information Systems Manager.

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

A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Organizations Participating Included:

A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

The Venue and Accommodation

L'Auberge Hotel & Casino
777 L'Auberge Ave
Lake Charles 70601
Louisiana

Featuring an on-site casino and live music venues, the L'Auberge Hotel and Casino in Lake Charles only 15 minutes drive from Lake Charles Airport, and less than 2 hours from Houston International Airport. The boutique-style guest rooms at L'Auberge Lake Charles have a flat-screen TV and an additional TV built into the bathroom mirror. Guests will also enjoy the comfort of a plush robe. Plenty of restaurant options, including a buffet, a steakhouse, a sports bar, grille and wine bar, and a café offer a wide variety of meal options for L'Auberge guests. Even the spacious casino floor can't contain all of the fun, wonder and glamour of L'Auberge Casino Resort! You'll find plenty of ways to pass the time in peerless style.with views of the Mississippi River. A fitness centre is available for relaxation. Self-parking is available to hotel guests at no extra charge. Valet parking is also offered.

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

Booking Your Accommodation

Special Room Rate for CIPRNA Delegates – $139 prpn (excl taxes)

Promo Code: **STORCH24A**

Book your hotel accommodation at the **L'Auberge Hotel & Casino** 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 STORCH24A to get your CIPRNA group booking rate.

Special Group Rate ends 18th February

We look forward to welcoming you to Lake Charles.

A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

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:

Ray Beauchamp
Americas
E: rayb@torchmarketing.co.uk
T: +1 559-319-0330

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

Sam Most
ROW
E: samm@torchmarketing.co.uk
T: +44 (0) 208 123 7909

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 - $14,950
- Gold Sponsor - $10,500
- SIlver Sponsor - $8,950
- Bronze Sponsor - $6,950
- Conference Proceedings Sponsor - $4,950
- Site Visit Sponsor - $4,500
- Delegate Folder Sponsor - $4,500
- Networking Reception Sponsor - $3,500
- Coffee Break Sponsor - $3,500
- Lanyard Sponsor - $3,500
- Badge Sponsor - $3,500

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' - $3,000
Table Top Exhibit 10'x10' - $4,950
Raw space with 1 x table and 2 x chairs, pipe and drape, electrical socket, wi-fi, 1 Exhibitor Delegate pass 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 10.2% LOUISIANA/LAKE CHARLES SALES TAX

A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Sponsors and Supporters:

We wish to thank the following organisations for their support and contribution to Critical Infrastructure Protection & Resilience North America 2024.

Platinum Sponsor:

TRUSTED COMPUTING GROUP

Supported & Co-Hosted by:

International Association of CIP Professionals

INFRAGARD MEMBERS ALLIANCE LOUISIANA

Silver Sponsors:

JCI | Security Products

ASSA ABLOY

HID

VITAL INTEGRATORS

Bronze Sponsors:

Genetec

SALVADOR TECHNOLOGIES

CLEARFORCE

CONSORTIUM NETWORKS

ECHODYNE

Executive Sponsor:

INSTITUTE FOR HOMELAND SECURITY

Networking Reception Sponsor:

milestone

Coffee Break Sponsor:

AXIS COMMUNICATIONS

Lanyard Sponsor:

CAPITOL Technology University

Supporting Organisations:

IACI

Help2Protect

ISIO

RS&RC

TIA Telecommunications Industry Association

Flagship Media Partner:

critical infrastructure PROTECTION AND RESILIENCE NEWS

Media Supporters:

Cyber Security Review

govCIO OUTLOOK

TSI TRANSPORT SECURITY INTERNATIONAL

World Security-index.com

Industrial Cyber

BIOMETRIC

grc outlook

BORDER SECURITY REPORT

Owned & Organised by:

TORCH

DELEGATE REGISTRATION FORM

EARLY BIRD SAVINGS

Book your delegate place by 12th February 2024 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 2024, 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 12th February 2024 ..... $195
- ☐ Paid on or after 12th February 2024 ..... $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 12th February 2024 ..... $195
- ☐ Paid on or after 12th February 2024 ..... $295

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

- ☐ Paid before 12th February 2024 ..... $495
- ☐ Paid on or after 12th February 2024 ..... $795

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

- ☐ Paid before 12th February 2024 ..... $245
- ☐ Paid on or after 12th February 2024 ..... $395

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

- ☐ Paid before 12th February 2024 ..... $100
- ☐ Paid on or after 12th February 2024 ..... $250

- ☐ **CITGO Site Visit** (delegates only) $50
  (Tues 12th March - includes return coach from hotel venue. Limited spaces available - book early to avoid disappointment)
- ☐ **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 12th March 2024.
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 12th February 2024. 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 - 10.2% 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