

critical infrastructure

PROTECTION AND
RESILIENCE **AMERICAS**

March 7th-9th, 2023
BATON ROUGE, LOUISIANA
A Homeland Security Event

Collaborating and Cooperating for Greater Security

For Securing Critical Infrastructure and Safer Cities

Co-Hosted & Supported by::



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



Gold Sponsor:



Leading the debate for securing America's critical infrastructure

Supporting Organisations:



Media Partners:





A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Welcome to the 4th 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, Baton Rouge on March 7th-9th, 2023.

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 conference in Baton Rouge, Louisiana, for what will be 3 days of exciting and informative discussions on securing North America's critical infrastructure.

The last few years have been some of the most challenging in our recent history. As we emerged from the Coronavirus pandemic, we saw the onset of a most regrettable and dreadful war between Russia and Ukraine and the obvious impact that has had on Global Peace and Security.

Critical infrastructure spans everything from transportation, energy systems and water to communications, healthcare, chemicals and many more. They underpin all the essential functions that keep a country and its economy running. Yet, they continue to face a myriad of threats from weather-induced phenomenon, physical attacks and malicious cyber activity, which can be instigated from across the globe by those individual and state actors seeking to disrupt or destroy the vital services that every country relies upon.

This is a critical time for all within our Infrastructure sectors, both natural and man-made disasters are here to stay. Our critical infrastructure is crucial to modern life. No matter what, we need these facilities and their systems to stay up and running, which means they must be prepared, protected and resilient if they come under any form of attack or fall foul of natural hazards.

Unfortunately, we all have to understand that the days of simple security measures are long gone, the dynamics have changed considerably and so to must our total approach to security and resilience. 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 an exciting

agenda lined up with some excellent speakers covering a wide range of important topics, presenting their thoughts on the way forward and their views on the current and emerging good practice that is in place across the world.

We are also delighted to be here in Baton Rouge with the support of a number of organisations, which include:

- InfraGard Louisiana
- Governor's Office of Homeland Security and Emergency Preparedness-Louisiana
- Mayor's Office of Homeland Security and Emergency Preparedness-Louisiana
- Regional representatives of CISA, TSA;
- The International Emergency Management Society;
- International Association of Certified ISAO's (IACI)

This is our 4th conference here in the United States and it will bring together leading stakeholders from across industry, operators, agencies and governments. This event will build on what we have delivered over the past few years and is specifically designed to challenge current thinking, stimulate debate and encourage your active participation across the sessions.

The exhibition taking place alongside the conference will be showcasing some of the latest technologies that are currently being utilised internationally within both the physical and cybersecurity environments across a range of infrastructure sectors.

I know you will find this a most rewarding and enjoyable event and I look forward to seeing you in Baton Rouge on the 7th to the 9th of March 2023.



John Donlon QPM FSyl



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 latest 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, FEMA, DISA, TSA 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

Join us in Baton Rouge, 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 7th	1.00pm to 7.30pm	Tuesday March 7th	8.00am to 6.00pm
Wednesday March 8th	9.30am to 5.30pm	Wednesday March 8th	8.30am to 5.00pm
Thursday March 9th	9.30am to 4.30pm	Thursday March 9th	8.30am to 4.00pm

REGISTER ONLINE AT WWW.CIPRNA-EXPO.COM

Register Online Today at www.ciprna-expo.com/onlineereg

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 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 7th, 2023

Register yourself and your colleagues as conference delegates by February 7th, 2023 and save with the Early Bird Discount. Registration details can be found at www.ciprna-expo.com/registration.

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

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)
 - Security Partners Forum (SPF)
 - Global Institute for CyberSecurity & Research (GICSR)

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 7th, 2023

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 8th, 2023

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: Power & Energy Sector Symposium

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

2:00pm-3:30pm - Session 4a: Communications Sector Symposium

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

4:15pm - 5:30pm - Session 5a: Critical Manufacturing & Logistics Sector Symposium

TRACK TWO

9:00am-10:30am - Session 2b: Crisis Management, Coordination & Communication

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: CBRNE Sector Symposium

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

4:15pm - 5:30pm - Session 5b: Government, Defence & Space Sector Symposium

Thursday March 9th, 2023

9:00am-10:30am - Session 6a: Mitigating Major Threats

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

11:15am - 12:30pm - Session 7a: Developing Resilience Strategies

9:00am-10:30am - Session 6b: Business and Community Perspectives and Private Sector Funding for Critical Infrastructure Preparedness

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

11:15am - 12:30pm - Session 7b: Technologies to Detect and Protect

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

2pm-3:30pm - Session 8: PANEL DISCUSSION: "The Last Mile" Community Roles in Critical Infrastructure and National Preparedness

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

4:30pm - Expo Close

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

8 | Register Online at www.ciprna-expo.com/onlineereg



A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Wednesday March 8th, 2023

WORKSHOPS ROOM

9:00am-10:30am - Session 2c: Global Cyber First Responder Workshop

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

11:15am - 12:30pm - Session 3c: Establishing a CIPR Community

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

2:00pm-3:30pm - Session 4c: The International Emergency Management Society Workshop

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

4:15pm - 5:30pm - Session 5c: TBC

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 Baton Rouge, 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

Exhibitor Showcasing in the Expo:

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



Register for your FREE Expo Pass
www.ciprna-expo.com/onlinereg



A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Tuesday March 7th

Conference Programme

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

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

Dr David Mussington, Executive Assistant Director for Infrastructure Security, Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA)

Clay Rives, MPA, LEM-P, Director, East Baton Rouge Parish | Mayor's Office of Homeland Security & Emergency Preparedness

Eric Rollison, Assistant Director risk analysis, resilience and recovery, CESER and DOE

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

Making a Business Case for Security: A Case Study - Daryle Hernandez; Scott Dunford; Shaina Wojciechowicz, Chief of the Interagency Security Committee; Senior Security Specialist; Economist, CISA

Cascading Effects - Mike Willis, Director of Emergency Management, State of Colorado

PPPs and Communities - Lester Millet, President, Infragard LA

Priority Capabilities to Bolster Resiliency - Dawn Manga, Associate Director Priority Communications, CISA

Achieving and Sustaining Critical Infrastructure Preparedness - Jeff Gaynor, President, American Resilience

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

**invited*





A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Wednesday March 8th

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?

Extreme Weather Impacts to Critical Infrastructure - Sunny Wescott, Lead Meteorologist - Extreme Weather Outreach, CISA

Vanessa Tibbits, Associate Special Agent in Charge, FBI
WMD program for CI - Jeffrey Hirsch & John Morse
WMD Program, FBI

Emerging Cyber Threats - Senior Representative, NSA*
AI Challenges for CI - Tom Roberston, The International Emergency Management Society (TIEMS)

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

11:15am-12:30pm - Session 3a: Power & Energy Sector 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.

Marisol Cruz Cain, Director IT & Cybersecurity,
Government Accountability Office (GAO)

Eric Rollison, assistant director risk analysis, resilience
and recovery CESER and DOE

**Leveraging Machine Learning to Improve Hazardous
Drilling Operations** - Joe Morgan, Segment
Development Manager - Critical Infrastructure, Axis
Communications

Darin Dillon, Senior Director Energy, LeneIS2

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

TRACK TWO

9:00am-10:30am - Session 2b:

Crisis Management, Coordination & Communication

Planning and preparation is the key to ensuring that CI and venue operators have the right equipment, processes and procedures in place to respond in the event of an emergency. Coordination and information sharing is essential for situational awareness and can improve the planning process. How do we better coordinate and co-operate to enhance protection and resilience.

**Data and Information Sharing for the Critical
Infrastructure Enterprise** - Carmen Zapata, Senior
Technical Advisor, Infrastructure Security Division, CISA

Critical Infrastructure Facility Protection Awareness -
Ron Martin, Capitol Tech University

George Markowsky, The International Emergency
Management Society

**The Response Recipe: Combining emergency
management, continuity, and cyber incident
response** - Keyaan J Williams, Managing Director, Cyber
Leadership and Strategy Solutions, 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.

Ronald Pavlik, Deputy Assistant Administrator, Transport
Security Administration

Challenges with Cybersecurity at Airports - Carissa
VanderMey, Sr Liaison to CISA and Cybersecurity
Coordinator - Security Operations, TSA

Physical Security Challenges at Airports - Arden
Hudson, Federal Security Director, TSA

Zach Albritton, Senior Special Agent, Union Pacific
Railroad Police

HPD Lt Christopher Smith, Harbor Police Department,
Port of New Orleans

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



critical infrastructure PROTECTION AND RESILIENCE AMERICAS

March 7th-9th, 2023

BATON ROUGE, LOUISIANA

A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Wednesday March 8th

TRACK ONE

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

Priority Telecommunications - Stay Connected When It Matters Most - Colleen Wright; Larry Clutts; Cathy Orcutt, Priority Telecommunications Area Representatives, CISA

Strategies to Counter 5G Threats and Secure the Cyber Domain - Melissa Ken, Assistant Professor of Law, US Air Force

Joshua Tannehill, Sr. Manager, Lumen Trust & Safety
Mike Regan, VP Business Performance,
Telecommunications Industry Association (TIA)

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

4:15pm-5:30pm - Session 5a: Critical Manufacturing & Logistics Sector Symposium



Critical Manufacturing Sector 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 with the need for resilient logistical operations, in order to ensure reliable and timely delivery is key to any thriving economy.

Joseph Booth, Sector Chief, Critical Manufacturing Sector, Infragrad LA

Bob Kolasky, Senior Vice President for Critical Infrastructure, Exiger

Risk Assessment and Hazard Mitigation Planning for Storage Tanks - Yangyang Wu, Director of Advanced Analysis, Roundtable Engineering Solutions

TBC

TRACK TWO

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



Sectors such as Chemicals, Nuclear and Water/Wastewater are as much at threat from an attack as a threat they pose that could include CBRNE agents in terrorist attacks against CI. The convergence of biological and cyber sector issues also characterises an evolving frontier in health security, and mitigation of such attacks is as much of a consideration as post attack resilience.

Chemical Sector Risk Management Agency Resources for Enhanced Security and Resilience - Dr Ashley Pennington, Chemical Engineer CISA

Joint Collaboration to Enhance Chemical Security - Dr. Ryan Donaghy, Deputy Branch Chief for Policy, Rulemaking, and Engagement, CISA

Buren (Ric) Morre, GOHSEP Intelligence Officer, Louisiana State Analytical & Fusion Exchange (LA-SAFE) Liaison & Amanda Ames, Chief Engineer, LDH/OPH/Engineering Services

TBC

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

4:15pm-5:30pm - Session 5b: Government, Defence & Space Sector Symposium



As we rely more and more heavily on satellites for communications, navigation, observation and security/defence, the requirement to ensure that space based systems are both secure and resilient becomes more urgent. Government networks and systems need to lead security and resilience across agencies and departments for confidence throughout the CI sectors and communities. What impact does the Government, Defence and Space based systems have as a growing role in CI resilience.

Advanced Persistent Threats: Threats to Public Safety Communications - Richard Tenney, Senior Advisor, Cyber, CISA Emergency Communications Division

Legal Aspects of Information Sharing and the National Plan to Secure Critical Infrastructure - Terence Check, Senior Counsel, CISA

Deborah Kobza, President, International Association of Certified ISOs (IACI)

Senior Representative, NASA*



A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Wednesday March 8th

Workshop One

9am-10.30am

Global Cyber First Responder Training & Certification

Moderator: Deborah Kobza, President, International Association of Certified ISAOs

Identify - Protect - Detect - Respond - Recover

Security Convergence - Advancing Critical Infrastructure Security Resilience

Requires Essential Public & Private Sector Coordination and Collaborative Security Response Across Physical, Cyber and Cyber-Physical Domains

This Workshop is a Defining Voice Opportunity to Participate and Benefit from:

- Appointment to the Global Security Resilience Alliance (GSRA)
- Defining Global Cyber First Responder Roles, Responsibilities, Competencies and Response Protocols - Supported by Training & Certification
- Alignment of Public & Private Physical, Cyber, and Cyber-Physical Response Protocols in Coordination and Collaboration with US DHS / Federal, State, Local, Tribal, Territorial Government / Fusion Centers, Law Enforcement, Critical Infrastructure Owners & Operators, Global CERTs, etc.
- Physical / Emergency Response & Cyber Response Cross-Training - Ensuring Threat and Incident Response is Focused from an All-Hazards Perspective
- Security Convergence Table-Top Exercise (Physical, Cyber, Cyber-Physical) - Being Developed by US DHS
- Access to Global Actionable Intelligence Information Sharing, Analysis and Response - Within and Across Critical Infrastructure Public & Private Sectors

Secure Communications - Patented Zero Trust Encrypted Communications Technology Developed for the CIA - Different DNS than the Public Internet

- OT Security Lab - Research / Training / Exercise

Workshop Two

11.15am-12.30am

Establishing a CIPR Community

Moderator: Jeff Gaynor, American Resilience

Because community-based Critical Infrastructure (CI) empowers the spectrum of American Life, the reliable provision community-based CI products and services are indisputably personal for all drawing a breath.

Accordingly, CI sectors are organized, built, and operated to symbiotically merge in American communities. It is therefore mandatory that community perspectives regarding their CI performance-based funding requirements be provided by community-based customers, CI providers, business leaders and local authorities and further, be continuously captured, triaged, and funded.

Doing so requires the timely, accurate, and actionable exchange of CI situational awareness information from American communities to both ends of Pennsylvania Avenue. Only with that information will the Nation be able



A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Wednesday March 8th

to coherently invest to lower CI target values, correct their consequence enabling and multiplying cyber-reliant condition, equalize prevention, continuity, response, and recovery investments and achieve ideal levels of CI protection, security, and operational resilience.

Accordingly, the panel will provide community and business-based CI perspectives and will introduce a private sector initiative to secure funding for continuous community-based CI modernization to ensure the safety, security, quality of life and future for this and generations of Americans to follow.

Workshop Three 2:00pm-3.30pm

The International Emergency Management Society Workshop

Moderator: Dr. Tom Robertson, TIEMS Regional Director for North America, and Dr. George Markowsky, President of TIEMS USA

TIEMS (www.tiems.info) is entering its 30th year as an international forum dedicated to sharing research, technologies, and best practices for disaster and emergency management. We convene international conferences, participate in research, technology, and development programs, and offer unique certifications in international emergency management, TQCTM and TQACTM.

In this CIPRNA workshop we will present a snapshot of the international community's perspective on EM, as presented at our TIEMS 2022 Annual Conference. We will then review three European research and development projects addressing pandemics, climate change, and security in smart cities. Finally, we will highlight TIEMS activities here in the USA.

We look forward to an interactive session - sharing perspectives, insights, and experiences with our colleagues.

The workshop will be presented by Dr. Tom Robertson, TIEMS Regional Director for North America, and Dr. George Markowsky, President of TIEMS USA.

Part 1 – International Perspectives from the TIEMS 2022 Annual Conference

Part 2 – Review of Three European Commission Projects in Disaster and Emergency Management

- **ASSET** - A project to develop better ways to communicate with and engage the public during pandemics. This pre-COVID project was launched in reaction to the poor results achieved by European government actions taken during the H1N1 pandemic
- **HERACLES** - A project to combine remote sensing, chemical analysis, and decision support tools to prioritize and manage activities for preserving cultural heritage sites endangered by climate change
- **IMPETUS** – A project using AI and other advanced tools to analyze smart city data such as CCTV video, social media, and communications networks, to improve public safety during large-scale urban events.

Part 3 – TIEMS USA Activities



A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Thursday March 9th

TRACK ONE

9:00am-10:30am - Session 6a:

Mitigating Major Threats

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 can we counter these emerging physical and cyber threats to minimise loss of service and financial impact?

Improvised Explosive Devices and Critical Infrastructure Protection - Douglas DeLancey, Chief, Strategy Branch, Office for Bombing Prevention

The Importance of Embedding Security into the Design of CNI Facilities - Sarah Jane Prew, Senior Security Consultant, Arup, UK

The Insider Threat - Catherine Piana, Secretary General, Help 2 Protect, Belgium

Implementing the NIST CSF - Glenda R. Snodgrass, President, The Net Effect, LLC

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

**11:15am-12:30pm - Session 7a:
Developing Resilience Strategies**

How to we develop and plan the best resilience strategies within our CI community? Through discipline in information sharing and making infrastructure preparedness personal, we can help to build resilience into our infrastructures that benefit the whole community.

The P.A.C.E. of Risk Society - Dr. William T. Spencer PhD, Deputy Associate Director of Operations, District of Columbia's Homeland Security and Emergency Management

Resiliency Benefits of a Holistic Identity - Charles Burton, Technology Director, Calcasieu Parish Government

The Health Analysis Research for Public Events (HARPE) Tool - Stephanie Jenkins, Cyber Security Analyst, Argonne National Laboratory

TBC

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

TRACK TWO

9:00am-10:30am - Session 6b:

Funding for CI, Community, Business, State and National Resilience-based Preparedness

America's critical infrastructure preparedness trajectory continues to decline. In an increasingly dangerous domestic and international environment, America must have, an objectively measurable, achievable, and sustainable critical infrastructure and by extension National preparedness condition – one built from Communities to Washington, DC. The biggest obstacle to the continuous modernization of America's community-based, and inextricably cyber-reliant critical infrastructures has been funding. In view of the foregoing, the panel will address business and community perspectives on CI preparedness and (via pre-recorded presentation), an historically and operationally proven initiative now before the US Congress: The creation of a community and state CI requirements driven, private sector organized and operated National Infrastructure Bank.

Chair: Jeff Gaynor, American Resilience

Jeff Gaynor, President, American Resilience

Minna LeVine, CEO/President, SMART Community Exchange

Tedra Cheatham, CECd, Executive Director, State Economic Competitiveness Louisiana Economic Dev.

Alphecca Muttardy, Member, National Infrastructure Bank Coalition, Former Senior Economist, International Monetary Fund

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

**11:15am-12:30pm - Session 7b:
Technologies to Detect and Protect**

What are some of the latest and future technologies, from ground surveillance, space based or cyber technology, to predict or detect the wide range of potential threats to CNI.

Secure Tomorrow Series: A Strategic Foresight Toolkit to Prepare for the Future - Noel Kyle, Program Lead, CISA

How Unified Physical Security Solutions Help You Thrive in Evolving Times - Stephen Homrighaus, Account Executive, Enterprise Markets, Genetec

Overcoming infrastructure security and response challenges - David Armstrong, vice president and general manager of North America government, transportation and defense for Hexagon's Safety, Infrastructure & Geospatial & Matt Sexton, Cybersecurity and IT Expert

TBC

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



A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Thursday March 9th

2pm-3:30pm - Session 8: PANEL DISCUSSION: “The Last Mile” Community Roles in Critical Infrastructure and National Preparedness

Given over 90% of US critical infrastructures are privately owned and operated, how do we make infrastructure preparedness objectively measurable and moreover, personal? The implementation of nationally comprehensive and compatible, objectively measurable and operationally proven solutions are required to correct situational awareness, information and requirements gaps between critical infrastructure sectors, operators and consumers to meet the the Presidential (PPD-21) infrastructure policy goals. ‘Communities’ are “The Last Mile” of critical infrastructure product and service delivery. The panel will focus on this reality and the means to actively engage America’s communities in informing and achieving America’s infrastructure and National preparedness goals.

Moderator: John Donlon QPM FSI

Clay Rives, MPA, LEM-P, Director, East Baton Rouge Parish | Mayor’s Office of Homeland Security & Emergency Preparedness

Jeff McKee, Regional Coordinator, CISA

Lester Millet, President, Infragrad LA

Euclid D. Talley, Branch Manager, Critical Infrastructure Protection, Governor’s Office of Homeland Security & Emergency Preparedness

Jeff Gaynor, President, American Resilience

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

Networking Reception

Tuesday March 7th

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



Daryle Hernandez

Chief, Interagency Security Committee (ISC), CISA

Mr. Daryle Hernandez serves as the Director of the Interagency Security Committee (ISC) in the Cybersecurity and Infrastructure Security Agency (CISA). In this role, he is responsible for implementing Presidential Executive Order 12977 to enhance the quality and effectiveness of security in, and the protection of buildings and non-military Federal facilities in the United States. He does this with and through the chief security officers and other senior executives from 64 Federal departments and agencies that make up the ISC membership. Prior to his arrival to CISA, Mr. Hernandez was an interagency senior advisor with a FEMA National Incident

Management Assistance Team where he deployed in support of incident response operations in Guam and South Carolina.

Prior to this, Mr. Hernandez led the Department of the Army's protection office responsible for synchronizing multiple programs to protect a workforce of 1 million located on over 100 federal installations and in 6,000 separate standalone facilities. His focus was on producing unity of effort across organizations and programs to include Anti-Terrorism, Physical Security, Law Enforcement, Emergency Management, Fire & Emergency Services, Operations Security, Continuity of Operations, Health Protection, and Computer Network Defense and Information Assurance.



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 Millett 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.



Deborah Kobza

President, International Association of Certified ISAOs (IACI) & Global Security Resilience Alliance (GSRA)

As President of the Global Security Resilience Alliance (GSRA) and the International Association of Certified ISAOs (IACI) including the IACI-CERT headquartered at NASA/Kennedy Space Center, FL, Mrs. Kobza serves as a security strategist, supporting operationalizing security resilience via strategic leadership and public and private national/international collaborative partnerships - supported by a global critical infrastructure public and private-sector actionable intelligence and defensive measures information sharing infrastructure (IACINet), security analysis, tools and technologies, OT Security Lab infrastructure, and coordinated response supported by the adoption of best practice (research, testing education).

Mission - Accelerating Security Resilience by Advancing Security Intelligence Information Sharing and Response within and across Public and Private Critical Infrastructure...Breaking Down Long-Standing Barriers and Silos.

Security Resilience Coordinated Response - Global Cyber First Responder Training & Certification, Alignment of Physical, Cyber and Cyber-Physical Response Protocols working in coordination and collaboration with US DHS/CISA, federal/state/local/tribal/territorial agencies, law enforcement/public safety, ISAOs/ISACs, academia, NGOs, and Associations.

Ms. Kobza helps support operationalizing ISAOs/ISACs - Working with public- and private-sector communities to operationalize critical infrastructure sector and sub-sector ISAOs and ISACs - Maritime & Port Security ISAO (MPS-ISAO), National Credit Union ISAO (NCU-ISAO), Mining & Metals ISAC (MM-ISAC), Population Health ISAC, Community Transportation ISAC, Wisconsin ISAO (WICTRA), Florida ISAO, Louisiana ISAO, Public Safety Threat Alliance (Law Enforcement, Public Safety), Smart Cities ISAO, Regional and Local ISAOs, etc.



Minna LeVine

Founder, Smart Community Exchange

Minna LeVine is the Founder of SMART Community Exchange and Chair of the SMART Community Council, USA and Nordic Business Council, USA. She is the Co-Chair of the American Infrastructure Resilience and National Preparedness Council (AIRNPC) and is the Editor-in-Chief of "SMART Community Review."

Educated in Finland, Switzerland, and the United States, Minna brings extraordinary experience and perspectives on business and community life and the application of both American and European technologies. To ensure the resilience-based preparedness of America's cyber-reliant critical infrastructures, Minna teams with critical infrastructure and financial service innovators, infrastructure operators, business and community leaders to capture their infrastructure performance requirements and spearhead investment in the deployment of SMART-R© (SMART + Resilient) Critical Infrastructures for the United States and its Allies.



A Homeland Security Event For Securing Critical Infrastructure and Safer Cities



Catherine Piana

Managing Director, Help2Protect SRL, Belgium

Catherine Piana is a Security and Insider Threat expert. For over 8 years, she has been the voice of Private Security in Europe and Aviation Security on an international level.

In her position of Director General for both the Confederation of European Security Services (CoESS) and Aviation Security Services Association – International (ASSA-i), she has led a number of security initiatives, advocacy campaigns, EU-funded projects, standardisation projects and various publications.

On behalf of CoESS, she was the coordinator of the EU-funded project AITRAP, which led to the creation of an e-learning platform on the Insider Threat in at the end of 2018, under the name of Help2Protect (H2P in short) with the support of Securitas, DHL and Palmyra Aviation Advisors. When the EU funds could no longer support the platform, Catherine and the AITRAP project manager, Hugo Lücke (Palmyra Aviation Advisors), took it over, updated and expanded it and set up the commercial company Help2Protect SRL.

Catherine holds a Masters Degree in Translation (ISTI, Université Libre de Bruxelles), an MBA, a certificate in Counter Terrorism (Leiden University), is a Master Practitioner in Neurolinguistic Programming (NLP), and a certified Trainer and Coach.



Cathy Orcutt

Priority Telecommunications Services Area Representative (PAR), CISA

Cathy Orcutt is the Priority Telecommunications Services Area Representative (PAR) for the CyberSecurity and Infrastructure Security Agency (CISA) for Regions 8 – CO, UT, WY, MT, SD, ND and 10 – AK, OR, WA, and ID.

Cathy assumed her responsibilities as a PAR in late 2019 after spending 30 years in the 911 Emergency Communications field as a dispatcher, lead dispatcher and PSAP Manager.

Cathy's responsibilities as a PAR are to support national leadership; federal, state, local, tribal and territorial governments; first responders; and other authorized national security and emergency preparedness (NS/EP) users on the value and use of Priority Telecommunications Services. Priority Telecommunications Services Area Representatives (PARs) work in the field, focused on expanding Government Emergency Telecommunications (GETS), Wireless Priority Services (WPS) and Telecommunications



Carmen Zapata

Sr. Technical Advisor, Infrastructure Security, CISA

Carmen Zapata, Sr. Technical Advisor, Data Analysis Research & Technology, CISA Infrastructure Division Ms. Carmen Zapata is a Senior Technical Advisor for Data, Analytics and Research Technology (DART) at the Cybersecurity and Infrastructure Security Agency (CISA) in the Infrastructure Security Division. CISA leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure. We connect our stakeholders in industry and government to each other and to resources, analyses, and tools to help them build their own cyber, communications, and physical security and resilience, in turn helping to ensure a secure and resilient infrastructure for the American people.

Prior to her role as Senior Technical Advisor, Ms. Zapata worked at CISA's National Risk Management Center as the Deputy Associate Director for Analysis, where she created the Data Analytics team and helped oversee several research and technology projects out of the National Infrastructure Simulation and Analysis Center (NISAC) to evaluate risks to the nation's critical infrastructure. Ms. Zapata has also supported other federal agencies such as the Department of Homeland Security's Countering Weapons of Mass Destruction Office and the U.S. Department of Agriculture, providing her expertise on modeling and simulation, systems engineering and supply chain management.



A Homeland Security Event For Securing Critical Infrastructure and Safer Cities



Jeff Gaynor
President
American Resilience

Jeff Gaynor is a National Thought Leader advocate for and practitioner of Critical Infrastructure (and by extension), Business, Community and National Resilience mindsets, metrics, methodologies and technologies. Jeff's National Security career spans better than a half-century. He is a retired Army Colonel and Silver Star recipient and Defense Intelligence Senior Executive. In his 30+ years of military service Jeff's assignments ranged from the foxhole as an Advisor to Vietnamese Territorial Forces; to Intelligence Officer and Counterintelligence Agent and Operations Officer to Intelligence Battalion Commander to service at the White House as the Communications Security Officer and an Alternate Military Aide to Presidents' Ronald Reagan and George H.W. Bush. As a Defense Department Civilian and Senior Intelligence Executive, Jeff served as the Principal Action Officer for creation of the Defense-wide Information Assurance Program. He directed Department of Defense (DoD) Year 2000 Operations and became DoD's first Principal Director for Security and Information Operations. In the immediate wake of 9/11, Jeff served as a Defense Intelligence Liaison Officer to the White House and with his assignment there, created and directed the Emergency Response Senior Advisory Committee (ERSAC) of the President's Homeland Security Advisory Council. Jeff transitioned the ERSAC to the U.S. Department of Homeland Security and created and directed the Homeland Security Advisory Council's (HSAC) Critical Infrastructure Task Force (CITF). The HSAC's January 2006 CITF Report and its principal recommendation to: "Promulgate Critical Infrastructure Resilience (CIR) as the top-level strategic objective – the desired outcome – to drive national policy and planning" stands as "The Foundational U.S. Government document on Critical Infrastructure Resilience." Jeff is the Immediate Past President and CEO of the InfraGard National Members Alliance, a Past President of the InfraGard Atlanta Members Alliance and is the President of American Resilience, LLC.



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.



Colleen Wright,
Priority Services Outreach and Acquisitions, CISA

Colleen Wright is the Priority Services Outreach and Acquisitions Specialist for the Cybersecurity and Infrastructure Security Agency (CISA). Her mission is to ensure Priority Services are available to all who could face challenging communications congestion in the course of their National Security/Emergency Preparedness role. She is a retired Army communicator, with over 27 years' experience in tactical, strategic, and commercial communications. In her final military role, she provided coordination support to DHS and the National Cybersecurity and Communications Integration Center (NCCIC) with the telecommunications and information technology industries to restore, repair, protect and sustain those capabilities in times of major disasters or events. She also previously worked as a PAR, championing the Priority Telecommunications Services in ten states in the West and Northwest.



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.



Kelly Murray
Associate Director for Chemical Security, CISA

Kelly Rae Murray is the Associate Director of Chemical Security at the Cybersecurity and Infrastructure Security Agency (CISA). CISA's Office of Chemical Security is responsible for the implementation of chemical facility security regulations and voluntary chemical security programs within the U.S. Department of Homeland Security.

As the Associate Director, Ms. Murray oversees the Agency's efforts to administer the Chemical Facility Anti-Terrorism Standards (CFATS) regulation, ChemLock program, and international initiatives.

Under the CFATS regulation, CISA assesses which US facilities are at high risk of terrorist attack or exploitation, and works collaboratively with owners and operators at high-risk sites to ensure security is in place to mitigate the security concerns posed by their chemicals of interest. Under the voluntary ChemLock program, launched in 2021, CISA provides chemical facilities with assessments, services, and tools to help them understand the risks they face and improve their chemical security posture.

Ms. Murray has been with CISA Chemical Security at DHS since January 2008, serving in a variety of roles, from program analyst to Compliance Branch Chief before serving in her current role. Her prior experience includes work with the U.S. Department of Defense (DoD) and Federal Emergency Management Agency (FEMA).



Mjr. Melissa Ken
Assistant Professor of Law, United States Air Force Academy

Major Melissa Ken is serves as an Assistant Professor of Law, United States Air Force Academy, Colorado Springs, Colorado where she is the Course Director for National Security Law. In addition to National Security Law, she also teaches Law for Air Force Officers, which is a required course for all 4,400 cadets. Major Ken received a direct commission as an Air Force Judge Advocate and entered active duty in May 2016. She graduated with a Bachelor of Arts from Messiah College in 2011 with honors. She then attended Rutgers School of Law and earned her

Juris Doctorate in May 2014. After graduating from Rutgers, she spent a year as a law clerk for a criminal judge serving with the New Jersey Superior Court, Vicinage 15.

She is admitted to practice law before the Supreme Court of Pennsylvania, the Supreme Court of New Jersey, and the United States Court of Appeals for the Armed Forces. Major Ken received her LL.M. in National Security and U.S. Foreign Relations Law, with highest honors, from The George Washington University Law School.



A Homeland Security Event For Securing Critical Infrastructure and Safer Cities



Scott Dunford
Senior Security Specialist, Interagency Security Committee (ISC), CISA

Mr. Scott J. Dunford serves as the Senior Security Specialist for the Interagency Security Committee (ISC) in the Cybersecurity and Infrastructure Security Agency (CISA). In this role, Mr. Dunford leads the foundational work of the ISC. Prior to joining CISA, Mr. Dunford was the Chief, Field Security Operations Branch for the United States Citizenship and Immigration Services (USCIS) leading a team of multi-disciplined security professionals implementing the agency physical security, information security, operations security, and identity management programs. He also served in the Headquarters, Department of Homeland Security (DHS), Physical Security

Division where he performed Security Compliance Reviews of DHS operational components. Additionally, Mr. Dunford served 25 years in the United States Air Force spending most of his career in the security forces. He concluded his military service in the rank of Chief Master Sergeant.



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.



William Spencer
Deputy Chief of Operations and Preparedness, District of Columbia's Homeland Security and Emergency Management Agency

Dr. Spencer has served in the field of public safety and administration since 2001 with multiple disciplines at various levels of government. His current position is the Deputy Chief of Operations and Preparedness for the District of Columbia's Homeland Security and Emergency Management Agency. In this role, he has direct oversight of five bureaus to include Preparedness, Logistics, Readiness & Response, Interoperability, and Safety & Security. Prior to that position, he served 13 years with the Pennsylvania Emergency Management Agency (PEMA) with the primary responsibility of supporting the 24 counties in western PA and other commonwealth agencies within all mission areas. Prior to PEMA, he was a municipal Police Officer and a Commissioned Intelligence Officer in the PA Army National Guard.

Dr. Spencer is also a career educator and subject matter expert for Higher Education Institutions in asynchronous and synchronous deliveries for Homeland Security, Emergency Management, Criminal Justice and Public Administration courses.



Stephanie Jenkins
Cyber Security Analyst- Critical Infrastructure, Public Events and Facilities, Argonne National Laboratory

Stephanie Jenkins is a Cyber Security Analyst at Argonne National Laboratory, focusing on critical infrastructure, as well as public events and mass gatherings. Her research focuses on both sporting and critical infrastructure, and the rising vulnerabilities and risks associated with potential cyber attacks. Previous research includes the growing threats of cybersecurity attacks in sports focusing on stadiums and arenas, fans, and the integrity of the game.

Her work aims to bring awareness to the importance of assessing modern threats and vulnerabilities in the public events realm, as both cyber and physical dependencies continue to evolve. Her work also includes building risk assessments focusing on the commercial facilities sector, as well as other critical infrastructure. Her educational background includes a BS in Sports Management from Indiana University and a MS in Safety, Security, and Emergency Management with a concentration in Homeland Security and Intelligence and National Security from Eastern Kentucky University.

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
Baton Rouge 70820
Louisiana



Featuring an on-site casino and live music venues, the L'Auberge Hotel and Casino in Baton Rouge only 30 minutes drive from New Orleans International Airport, and 20 minutes from Baton Rouge Airport.

The boutique-style guest rooms at L'Auberge Baton Rouge have a flat-screen TV and an additional TV built into the bathroom mirror. Guests will also enjoy the comfort of a plush robe.

Baton Rouge L'Auberge has a refreshing rooftop swimming pool with poolside cabanas and a full bar

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.

Book your hotel accommodation directly using the special link at www.ciprna-expo.com/accommodation



Accommodation

Special Room Rate for CIPRNA Delegates – \$124 prpn
 INCLUDING Continental Breakfast (excl taxes)

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

Special Group Rate ends 21st February

We look forward to welcoming you to Baton Rouge.





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
UK and ROW

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

Sam Most

Mainland Europe & Turkey
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 - \$12,500
- Gold Sponsor - \$8,950
- Silver Sponsor - \$6,950
- Bronze Sponsor - \$4,950
- Conference Proceedings Sponsor - \$3,950
- Delegate Folder Sponsor - \$3,950
- Networking Reception Sponsor - \$2,950
- Coffee Break Sponsor - \$2,950
- Lanyard Sponsor - \$2,950
- Badge Sponsor - \$2,950

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' - \$2,500

Table Top Exhibit 10'x10' - \$4,500

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 9.95% LOUISIANA/BATON ROUGE 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 2023.

Gold Sponsor:



Supported & Co-Hosted by:



Silver Sponsors:



Bronze Sponsors:



Flagship Media Partners:



Coffee Break Sponsor:



Conference Proceedings Sponsor:



Supporting Organisations:



Media Supporters:



Owned & Organised by:



March 7th-9th, 2023
BATON ROUGE, LOUISIANA

DELEGATE REGISTRATION FORM

EARLY BIRD SAVINGS

Book your delegate place by 7th February 2023
and save with the Early Bird rate

REGISTRATION IS SIMPLE

1. Register online at www.ciprna-expo.com/onlinereg
2. Complete this form and email to:
ciprna@torchmarketing.co.uk
3. Complete this form and fax to +44 (0) 872 111 3210
4. Complete this form and mail to:
CIPRE 2022, 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)

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 7th March 2023.

Substitutions/Name Changes: You can amend/change a delegate prior to the event 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 7th February 2023. Regrettably 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

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 7th February 2023 \$195
☐ Paid on or after 7th February 2023 \$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 7th February 2023 \$195
☐ Paid on or after 7th February 2023 \$295

COMMERCIAL ORGANISATIONS Individual Full Conference

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

- ☐ Paid before 7th February 2023 \$495
☐ Paid on or after 7th February 2023 \$795

Individual Day Delegate

(includes access to conference on the day, coffee breaks and lunch on the day)

- ☐ Paid before 7th February 2023 \$295
☐ Paid on or after 7th February 2023 \$395

Attending on: ☐ 7th March ☐ 8th March ☐ 9th March

Exhibitor Full Conference

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

- ☐ Paid before 7th February 2023 \$245
☐ Paid on or after 7th February 2023 \$395

Student Full Conference

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

- ☐ Paid before 7th February 2023 \$100
☐ Paid on or after 7th February 2023 \$250

☐ Conference Proceedings only \$495

☐ EXHIBITION ONLY FREE

(includes access to exhibition floor only)

PAYMENT DETAILS

(METHOD OF PAYMENT - Conference fees include Sales Tax at 9.95%.)

☐ 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 fax to +44 (0) 872 111 3210 or email to ciprna@torchmarketing.co.uk