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.

Leading the debate for securing America’s critical infrastructure
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.


**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 again 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 for 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 Doubletree by Hilton, New Orleans Airport on February 1st-3rd, 2022.

Follow us:
Dear Friends and Colleagues,

Collaborating and Cooperating for Greater Security

It gives me great pleasure to invite you to join us at Critical Infrastructure Protection and Resilience North America in New Orleans, Louisiana, for what will be 3 days of exciting and informative discussions on securing North America’s critical infrastructure.

Following the event’s postponement due to the Coronavirus outbreak, this situation highlights the urgent needs for our critical infrastructure to be prepared and resilient from multiple attack vectors, whether natural disaster, man-made or from terrorist attacks and the increasing cyber threats and Ransomware attacks.

This is our 3rd event in North America, which complements our Europe and Asia editions for this important topic of discussion.

We are delighted to be here with the support of InfraGard Louisiana and the New Orleans Office of Homeland Security & Emergency Preparedness, as well as other supporting organisations.

As you are all aware a nation’s critical infrastructure provides the essential services that underpin society and are a significant contributor to economy, security, and health. Rapid globalization has presented us all with an abundance of economic opportunities but also a growing number of interconnected and diverse threats. The risk environment affecting critical infrastructure is both complex and uncertain. Threats, vulnerabilities and consequences have all evolved over the past decade and infrastructure that has long been subject to the dangers associated with physical threats and natural disasters are now increasingly exposed to cyber risks which stems from the growing integration of information and communications within their operations.

So the days of simple security are long gone, the dynamics are changing and so too must our total approach to security and resilience.

There is, therefore a continual need to review, develop and update policies, practices 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.

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.

The Expo will be showcasing some of the latest technologies, both for physical and cybersecurity environments for your CI.

I know you will find this a most rewarding and enjoyable event and I look forward to seeing you in New Orleans, for the next in-person discussion on February 1st-3rd, 2022, where we will ensure a safe and Covid compliant environment.

John Donlon QPM FSyI
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 into 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:
Neil Walker
Events Director
T: +44 (0) 7725 318601   |   F: +44 (0) 872 111 3210
E: neilw@torchmarketing.co.uk

Who Should Attend

Critical Infrastructure Protection and Resilience North America is for:

- Police and Security Agencies
- DHS, FEMA, DISA 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/C00/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 New Orleans, 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.”
Schedule of Events

Tuesday February 1st, 2022
1:00pm - Exhibition Opens
2:00pm-3:30pm - Opening Keynote Session
3:30pm-4:00pm - Networking Coffee Break
4.00pm-5:30pm - Session 1: Strategies in CI Protection & Resilience

Wednesday February 2nd, 2022

**CRITICAL INFRASTRUCTURE PROTECTION / PHYSICAL SECURITY TRACK**
9:00am-10:15am - Session 2a: Emerging Threats For Critical Infrastructure
10:15am-11:00am - Networking Coffee Break
11:00am - 12:30pm - Session 3a: Countering the Emerging Threats - Security, Risk & Disaster Mitigation
12:30pm-2:00pm - Delegate Networking Lunch
2:00pm-3:30pm - Session 4a: The Developing Cyber Threat Environment
3:30pm-4:15pm - Networking Coffee Break
4:15pm - 5:30pm - Session 5a: Securing the Physical CI Asset
5:30pm - Networking Reception in Exhibition Hall

**CRITICAL INFORMATION INFRASTRUCTURE PROTECTION / CYBER SECURITY TRACK**
9:00am-10:15am - Session 2b: Cybersecurity Legislation, Standards & Best Practice
10:15am-11:00am - Networking Coffee Break
11:00am - 12:30pm - Session 3b: The Developing Cyber Threat Environment
12:30pm-2:00pm - Delegate Networking Lunch
2:00pm-3:30pm - Session 4b: Strategies and Collaboration in Cyber Defence
3:30pm-4:15pm - Networking Coffee Break
4:15pm - 5:30pm - Session 5b: IT OT Security and Safeguarding Against Cyber Threats

Thursday February 3rd, 2022
9:00am-9:45am - Session 6: Growth in Interoperability Between Critical Infrastructure Sectors and Enhancing Cross Industry Resilience
9:45am-10:30am - Session 7: Crisis Management, Coordination & Communication
10:30am-11:15am - Networking Coffee Break
11:15am - 12:30pm - Session 8: Operationalizing Critical Infrastructure Resilience
12:30pm-2:00pm - Delegate Networking Lunch
2:00pm-3:30pm - Session 9: PANEL DISCUSSION: The cyber-physical security challenge
3:30pm-4:00pm - Review, Discussion and Conference Close
4.30pm - Expo Close
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, FEMA, 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 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 January 15th, 2022
Register yourself and your colleagues as conference delegates by January 15th, 2022 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:

- 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
Tuesday February 1st

Conference Programme

2:00pm-3:30pm - OPENING KEYNOTE
Chair: John Donlon QPM, FSI
*invited
International adviser on security intelligence

Dr David Mussington, Assistant Director, CISA,
US Department of Homeland Security (DHS)*

Ret. Colonel Terry Ebbert
Director of Public Safety, City of New Orleans

TBC

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

4:00pm-5:30pm - Session 1: Strategies in CI Protection & Resilience
The ability to adapt to changing conditions and prepare for the unexpected will help us more rapidly recover from disruption. Resilience against changing threats, whether cyber or physical, is essential for CI to ensure mitigating economic impacts of disruption. What are the latest ideas and plans in developing resilience strategies? How can we best identify and manage risk and how do we best apply system-thinking to strengthen critical infrastructure resilience?

Chair: John Donlon QPM, FSI

National infrastructure Protection Plan (NIPP) - Jacob Anderson, Strategy Branch Chief, CISA/ISD

Brian Harrell, VP & Chief Security Officer, AVANGRID

Securing the Nations Largest Tonnage Port though Public Private Partnerships - Lester Millet, Safety Agency
Risk Manager / FSO Workgroup Chairman, Port of South Louisiana & Infragard Louisiana President

Evaluating Supply Chain Resilience - Mark Scott, Critical Infrastructure Specialist, District of Columbia Homeland Security and Emergency Management Agency

Risk, Reliance and the Resilience Imperative - Jeff Gaynor, President, American Resilience

A Decision Analytic Approach to Electric Infrastructure Resilience - Frédéric Petit,
Principal Infrastructure Analyst, Argonne National Laboratory

*TBC

Critical Infrastructure Protection & Resilience North America - www.ciprna-expo.com | 9
Wednesday February 2nd

**Critical Infrastructure Protection / Physical Security Track**

9:00am-10:30am - Session 2a:
Emerging Threats For Critical Infrastructure
The ever changing nature of threats, whether natural, through climate change, or man-made through terrorism activities and insider threats, means the need to continually review and update policies, practices and technologies to meet these growing demands. But what are those emerging threats and how can we identify, monitor and manage their levels of potential damage?

Ruth Christensen, Analyst, NCTC, FBI
Steve Zeringue, WMD Co-ordinator, FBI

Terrorism: Impact of Global Pandemic Heightening Risk Factors for Insider Threats - Andrew McLaughlin, Analyst, National Counterterrorism Center & Andrew Andell, Analyst, National Counterterrorism Center (NCTC)

Lauren Nash, Warning Coordination Meteorologist, National Weather Service/NOAA

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

11:15am-12:30pm - Session 3a:
Countering the Emerging Threats - Security, Risk & Disaster Mitigation
Being prepared for the changing threat environment can benefit greatly in mitigating its impact on infrastructure or crowded places, ensuring resilience, safety and security. How can we counter these emerging threats to minimising loss of service and financial impact?

Protecting Your Critical Infrastructure from Improvised Explosive Device Threats - Doug Delancey, Branch Chief, Counter IED Strategy, Integration & Comms, Office For Bombing Prevention, CISA

Countering UAS Threats - George Rey (InfraGard Louisiana BoD / Aviation Sector Chief)

HUMINT threats to organizational cybersecurity - John Bryk, Downstream Natural Gas ISAC

Don Davis, Section Chief - International Port Security Program, U.S. Coast Guard*

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

**Critical Information Infrastructure Protection / Cyber Security Track**

9:00am-10:30am - Session 2b:
Cybersecurity Legislation, Standards & Best Practice
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.

Starting the Journey: Cyber Incident Management Planning - Deron T. McElroy, Chief of Cybersecurity Services, CISA

Cybersecurity Resilience lifecycle - threat and defensive measures intel information sharing within and across sectors (government and industry), and the Cyber First Responder initiative - Debra Kobza, President, ISAOs

Improving Cybersecurity Posture Using the UFC 4-010-06 - Dr. Jeffrey (Jeff) Struik, Cyber Strike Solutions, LLC
Col Kenny Donnelly - Louisiana Cyber Commission*

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

11:15am-12:30pm - Session 3b:
The Developing Cyber Threat Environment
The ability to monitor the cyber threats to CNI can greatly assist the operators and agencies better prepare their defences against cyber attacks on systems and information/data. What is the latest strategic perspective on cyber monitoring and cyber defences for enhancing CIIP?

Securing Transportation’s Critical Infrastructure - Guerry Bruner, Assa Abloy

Defending Against OT Red Button Capabilities In Critical Infrastructure - Barak Perelman, CEO, Indegy
Robert Thibault, Supervisory Special Agent, FBI / InfraGard Louisiana
Adam Brickeen, IT & Security Chief, City of New Orleans Office of Homeland Security & Emergency Preparedness*

12:30pm-2:00pm - Delegate Networking Lunch
Wednesday February 2nd

**CRITICAL INFRASTRUCTURE PROTECTION / PHYSICAL SECURITY TRACK**

2:00pm-3:30pm - Session 4a:
**Methodology, Modelling, Simulation & Machine Learning**
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 modelling and methodology? What role can machine learning play in building more accurate simulation?

- The Emerging Role of Modeling and Simulation in Security Assessments and Design - Ben Eazzetta, CEO, ARES Security Corporation
- Multi-Asset and System Assessment - David Dickinson, Infrastructure Assurance Program Manager, Argonne National Lab.
- Use of GIS Capabilities and Huff Modeling to Estimate the Geographic Extent of Infrastructure Cascading Failures - Scott Schlueter, GIS Analyst, Argonne National Lab.
- Multi-Hazard Early Warning Systems and Building Community Resilience - Ron Fisher, Director, Infrastructure Assurance and Analysis Division, Idaho National Lab.

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

4:15pm-5:30pm - Session 5a:
**Securing the Physical CI Asset**
The physical infrastructure asset requires just as much focus from natural disasters, terrorist or man-made threats. Ensuring our assets are protected and resilient ensures continuity of supply and service, so what technologies are emerging to secure physical environments?

- An Inside Job: Protecting Chemical Facilities from Insider Exploitation - Todd Klessman, Deputy Associate Director, CISA
- The Importance of Embedding Security into the Design of CNI Facilities - Sarah-Jane Prew, Security Consultant, Arup
- Low-cost, Short-range Radar’s Role in a Safer, More Secure Critical Infrastructure Environment - Joe Morgan, Business Development Manager-Critical Infrastructure, North America, Axis Communications
- Preparation and prevention of physical attack on your CI - Roy Smith, President, Viking Tactical Security

**CRITICAL INFORMATION INFRASTRUCTURE PROTECTION / CYBER SECURITY TRACK**

2:00pm-3:30pm - Session 4b:
**Strategies and Collaboration in Cyber Defence**
To prevent catastrophic disruption or collapse of critical infrastructure CNI operators must develop the strategies, procedures, controls and co-operation to ensure resilience against cyber threats and attacks.

- Cyber Resilience: Keys to Protecting & Sustaining Critical Services - Deron T. McElroy, Chief, Cybersecurity Services, Region VI, CISA
- A Case Study in Hacking Critical Infrastructure - Steve Povolny, Head of Advanced Threat Research, McAfee
- Modeling and Spatial-Temporal Analysis of Cyber-Physical Impacts - Tim Klett, Cybersecurity Researcher, Idaho National Laboratory
- Harnessing the Power of Apprenticeship to Bridge the Cybersecurity Workforce Gap - Dr Marcus Rogers, Assistant Dean for Cybersecurity Initiatives, Fellow of the American Academy of Forensic Sciences (AAFS)

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

4:15pm-5:30pm - Session 5b:
**IT OT Security and Safeguarding Against Cyber Threats**
As more critical infrastructure becomes connected to the web, exposing IT and OT systems to cyber attack, what emerging technologies can assist in disrupting threats?

- Time FireWall - securing Critical Infrastructures against GPS Jamming and Spoofing attacks - David Fagelson, VP International Sales, AccuBeat
- Proactive OT Cyber Maintenance - Act Before the Breach - Marty Edwards, VP, Operational Technology Security, Tenable
- Why Device-Level Security is the Surest Way to Safeguard Critical Infrastructures - Yanir Laubshtein, VP, Cybersecurity & Industry, NanoLock Security
- A vision for tomorrow’s critical infrastructure security - Stephen Homrighaus, Account Executive, Enterprise, Genetec

5:30pm-7:30pm - Networking Reception in Exhibit Hall
Thursday February 3rd

9:00am-9:45am - Session 6: Growth in Interoperability Between Critical Infrastructure Sectors and Enhancing Cross Industry Resilience

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?

Chair: John Donlon QPM, FSI

Infrastructure Interdependency Assessment to Inform Resilience Investments
Paul Lewis, Program Lead, Argonne National Laboratory

A converged view of Industrial Control System Security - Ron Martin, CPP, CPOI, Professor of Practice, Capitol Technology University

9:45am-10:30am - Session 7: Crisis Management, Coordination & Communication

Session sponsored by: Government Technology & Services Coalition (GTSC)

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.

Chair: Kristina Tanasichuk, Founder & CEO, Government Technology & Services Coalition

Dr. Christopher Rodriguez, Director of Homeland Security and Emergency Management for the city of Washington, DC, USA

Chauncia Willis, Co-Founder and Chief Executive Officer, Institute for Diversity & Inclusion in Emergency Management

Creating an Emergency Management and Preparedness Program
Stephanie Murphy, Vice President, Resiliency and Critical Infrastructure Programs, Tidal Basin Government Consulting

Managing Your Response When Incidents Arise - Enterprise Incident Management for Critical Infrastructure - Marc Whalen, Global Vice President of Sales, Enterprise Incident Management (EIM), Qognify

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

11:15am-12:30pm - Session 8: Realities and the Resilience Imperative

America is the most cyber-reliant nation on the planet. Global predators recognize this self-inflicted condition and are very successfully exploiting it. The immediate and looming consequences of America’s reliance on technologies it has been unable to “secure” grow by the millisecond. Through predators’ eyes, America’s reliance on cyberspace is its Achilles Heel. Seven years after its post-Katrina introduction, “Critical Infrastructure Security and Resilience” (CIR) finally became America’s goal. Despite this, CIR remains conspicuous by its absence. To correct its increasingly exploitable and perilous critical infrastructure and national preparedness trajectories, the panel will offer the objectively measurable, performance-based means to achieve and sustain CIR for this and generations of Americans to follow.

Chair: Jeff Gaynor, President, American Resilience

Rob Cheng, CEO, PC Matic

Minna LeVine, Founder, SMART Community Exchange

Keyaan Williams, Founder and Managing Director of CLASS-LLC

12:30pm-2:00pm - Delegate Networking Lunch
Thursday February 3rd

2pm-3:30pm - Session 9: PANEL DISCUSSION: The cyber-physical security challenge
How do we address the rapidly converging cyber-physical security space?

Cyber attacks and Ransomware are becoming real issue and concern, where Colonial Pipeline and Solar Winds are recent prime examples. These cyber attacks are having an increasing impact on the physical assets infrastructure, requiring greater collaboration in the cyber-physical domain to better protect critical infrastructure. The strategy of ransomware cyber attacks on critical infrastructure has wider implications across other infrastructure services, and a broader economic impact on, for example, the price of petrol and oil, or panic purchasing from stores. Such cyber attacks, of which Ransomware is most common at the moment, should be a concern to us all. Are these State sponsored cyber hacks with the objective to disrupt, spread miscommunication and gather intelligence, or professional criminal organisations sponsored looking to make ‘easy money’ from creating the threat of economic harm? The interdependencies of our infrastructures means that such attacks are very difficult to isolate to the single asset. In this interesting, interactive panel discussion, we explore what happens in these cyber attacks, what lessons should be learned, how they can be prevented, as well as discuss how we can build better cyber-physical security and resilience into infrastructure networks. What is the impact on non-cyber, physical and resilience? Who should take responsibility and how can government, agencies, operators and the supply chains better collaborate to mitigate the next disastrous attack?

Moderator: John Donlon QPM FSI
Deron T. McElroy, Chief, Cybersecurity Services, Region VI, CISA
Brian Harrell, VP & Chief Security Officer, AVANGRID
Marco Ayala, Director, Director Industrial Control Systems Security, InfraGard Sector Chief, 1898 & Co., Burns & McDonnell
John Bryk, Downstream Natural Gas ISAC
TBC

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

Networking Reception

Wednesday February 2nd
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.
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.
Dr. Christopher Rodriguez  
Director of Homeland Security and Emergency Management for the city of Washington, DC

Dr. Christopher Rodriguez is the Director of the Homeland Security and Emergency Management Agency (HSEMA). In this role, Dr. Rodriguez serves as the Homeland Security Advisor and State Coordinating Officer for the District of Columbia. He also is the State Administrative Agent for all homeland security federal grants funding for the District and the National Capital Region which includes parts of Northern Virginia and Maryland.

Prior to HSEMA, Dr. Rodriguez served as Director of New Jersey’s Office of Homeland Security and Preparedness from 2014-17, where he led statewide strategies, policies, and operations on counterterrorism, resiliency, and cybersecurity.

Following the terrorist attacks of September 11, 2001, he joined the Central Intelligence Agency (CIA), where he became a senior analyst in its Counterterrorism Center. In this position, he monitored terrorist groups in the Middle East and South Asia, closely collaborating with U.S. Intelligence Community partners at the federal, state, and local levels to identify and counter persistent threats to the United States and its allies. During his time at the CIA, Dr. Rodriguez also oversaw an analytic unit that handled global economic and energy security, as well as related counterintelligence and cyber threats. From 2009-11, while deployed at the U.S. Embassy in Brussels, Dr. Rodriguez was a key U.S. interlocutor with the European Union during the height of the Euro crisis.

Brian Harrell  
VP & Chief Security Officer, AVANGRID

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 companies physical and cybersecurity, security compliance, enterprise risk governance, and fire protection 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 Assistant Director for Infrastructure Security at the U.S. Cybersecurity and Infrastructure Security Agency (CISA). Brian has spent time during his career in the US Marine Corps and various private sector agencies with the goal of protecting the United States from security threats.

Deron McElroy  
Chief Of Cybersecurity Services, Cybersecurity And Infrastructure Security Agency, Region VI

Deron McElroy is Chief of Cybersecurity Services for Cybersecurity and Infrastructure Security Agency (CISA) Region VI. He leads a team of Cybersecurity Advisors focused on enhancing our Nation’s cyber resilience. Deron’s team is available to help critical infrastructure owners and operators improve their cybersecurity posture, better manage cyber risk, and measure themselves against the NIST Cybersecurity Framework.

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

As IACI’s President and Co-Founder, Mrs. Kobza serves as a strategist and ensures IACI’s vision, mission, programs and services are fulfilled by providing leadership and national/international outreach establishing strategic partnerships to enable global cybersecurity information sharing and coordinated response, and to support the formation and sustainability of Information Sharing & Analysis Organizations (ISAOs).

Deborah’s 30+ years of experience and expertise in the areas of strategic alignment of business/technology domains, governance, cybersecurity, IV&V quality assurance, technologies, workforce education and applied research and implementation of proven best practices for public- and private-sector organizations, continue to contribute to critical infrastructure protection.


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.

Andrew McLaughlin  
Analyst, National Counterterrorism Center (NCTC), USA

Andrew McLaughlin is an analyst with the US National Counterterrorism Center (NCTC), covering terrorist threats to critical infrastructure. Andrew has worked on counterterrorism issues for most of his more than 15 years in the Intelligence Community, including more than a decade working at NCTC as an analyst and manager. Additionally, Andrew served as NCTC’s Houston-based Regional Representative from 2017-20, engaging federal, state, local, and private sector partners from Texas, Oklahoma, Louisiana, Arkansas, and Mississippi, including many in critical infrastructure fields.

16 | Register Online at www.ciprna-expo.com/onlinereg
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.

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.

Mark Scott
Critical Infrastructure Specialist, District Of Columbia Homeland Security And Emergency Management
Mark Scott is Critical Infrastructure Specialist for the District of Columbia’s Homeland Security and Emergency Management Agency. Mark’s career spans over 40 years in risk management in the public, private, and nonprofit sectors. His experience includes professional engagement in critical infrastructure protection and resilience with recent emphasis on supply chain risk management. For the District of Columbia, Mark leads a program to strengthen security and resilience of critical infrastructure in the Nation’s capital against all hazards. The program focuses on improving understanding of risk across all infrastructure sectors, applying that knowledge to inform decision-making and resource allocation, and helping infrastructure owners and operators and District response agencies build preparedness capability. Mark holds a master’s degree in Urban and Regional Planning from the University of Pittsburgh and is a member of the U.S Department of Homeland Security’s State, Local, Tribal and Territorial Government Coordinating Council (SLTTGCC).
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.

Stephanie Murphy,
Assistant Vice President, Resiliency and Critical Infrastructure Programs,
Tidal Basin Government Consulting

Ms. Stephanie Murphy is the Assistant Vice President for Preparedness, Resiliency, and Emergency Management for Tidal Basin Government Consulting. She leads a team of professionals in efforts to provide all-hazards, emergency management and preparedness services to Critical infrastructure provides and state and local jurisdictions. Ms. Murphy, a Certified Emergency Manager (CEM®), has over 18 years of experience in the areas of program development and project management in the Emergency Management and Transportation industries.

As the first Emergency Management and Preparedness Manager for the Metropolitan Washington Airports Authority in Washington, D.C., Stephanie developed a transportation emergency management and preparedness program from the ground up, focusing on strategic, incident and event planning; preparedness, response and recovery; corporate business continuity; training and exercising; and, identifying and implementing solutions for dynamic airport issues.

Prior to her Airports Authority tenure, Ms. Murphy was the National Planning Section Chief with FEMA as well as an International Crisis Management Trainer with the U.S. Department of State. Ms. Murphy also spent several years at the local level responding to countless emergencies and events, developing local and regional plans, serving in and Directing EOCs, and building resiliency in communities through planning, training, exercise and preparedness programs.
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.

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.

John Bryk
Cyber And Physical Threat Intelligence Analyst, DNG-ISAC, USA

Cyber and Physical Threat Intelligence Analyst John Bryk retired from the U.S. Air Force as a colonel after a 30-year career, last serving as a military diplomat in central and western Europe and later as a civilian with the Defense Intelligence Agency. Currently responsible for the operation of the Downstream Natural Gas Information Sharing and Analysis Center (DNG-ISAC), Colonel Bryk monitors and analyzes threats to natural gas across the United States and Canada. He holds, among other degrees, an MBA, an M.S. in Cybersecurity, and an M.A. in Business and Organizational Security Management.

Colonel Bryk is an internationally recognized Industrial Control Systems cybersecurity and intelligence speaker and has contributed to the President’s Cybersecurity Solarium Commission as a Subject Matter Expert.
Marc Whalen  
**Global Vice President of Sales, Enterprise Incident Management, Qognify**

The security of our nations’ critical infrastructure systems cannot be understated. Without the inability to properly manage any incidents that arise, critical infrastructure organizations face major risks. Marc Whalen, Qognify’s Global Vice President of Enterprise Incident Management (EIM) Sales, will be joining Critical Infrastructure Protection and Resilience to explore this topic. He will discuss the significant impact that access to real-time data and a robust EIM plan can make have on your continuity of operations and be vital in avoiding costly financial implications. Marc will also explore the importance for EIM systems to seamlessly and accurately address regulatory requirements such as NERC SIP, TSA, FAA and HIPPA.

Marc Whalen has been with Qognify since 2006, working in a variety of roles from regional sales to managing sales teams in the Eastern US and Latin America. Prior to joining Qognify, Marc held sales and management positions at organizations such as Siemens Building Technologies and Onity. Marc has 25 years of experience in the security industry and has a Bachelor’s of Science in Business from the University of Florida.

Dr. Marc Rodgers  
**Assistant Dean For Cybersecurity Initiatives, Fellow Of The American Academy Of Forensic Sciences (AAFS)**

Dr. Marc Rogers is a Professor, Assistant Dean for Cybersecurity Initiatives, Fellow of the American Academy of Forensic Sciences (AAFS) and Fellow - Center for Education and Research in Information Assurance and Security (CERIAS). Dr. Rogers is the Editor-in-Chief of the Journal of Digital Forensics Security & Law (JDFSL), and a member of the Board of Directors of the AAFS. His research interests include applied cyber forensics, psychological digital crime scene analysis, and cyber terrorism. Dr. Rogers is a frequent speaker at international and national conferences, and guest lectures at various universities throughout the world.

Marty Edwards is a globally recognized Operational Technology (OT) and Industrial Control System (ICS) cybersecurity expert who collaborates with industry, government and academia to raise awareness of the growing security risks impacting critical infrastructure and the need to take steps to mitigate them.

As Vice President of Operational Technology Security at Tenable, Edwards works with government and industry leaders throughout the world to broaden understanding and implementation of people, process and technology solutions to reduce their overall cyber risk.

Prior to joining Tenable in 2019, Edwards—a 30-year industry veteran—served as the Global Director of Education at the International Society of Automation (ISA). While at ISA, he was recognized by his industry peers with the SANS ICS 2019 Lifetime Achievement Award. Prior to ISA, Edwards was the longest-serving Director of the U.S. Department of Homeland Security’s Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).
Marco Ayala
Director Industrial Control Systems Security, InfraGard Sector Chief
1898&Co, Burns & McDonnell

Marco (Marc) Ayala is a process automation professional with over 25 years of experience working in petrochemical facilities, where he designed, implemented, and maintained their process instrumentation, automation systems, and process control networks. Currently, the director and ICS cybersecurity section lead at 1898 & Co. (part of Burns & McDonnell), Marco has expertise with safety systems, advanced process control, enterprise historians, and industrial network security, where he worked with enterprise IT to implement a corporate PCN security solution. He is active in cybersecurity efforts for the oil and gas, maritime port, offshore facilities, and chemical sectors, working alongside federal, local, and state entities for securing the private sector.

Marco is very active in ISA and is a 20-year member. He is a Senior member and a certified cyber instructor for ISA and a member contributor of the AMSC Gulf of Mexico (GOM) cybersecurity panel, InfraGard member, Chief of the Maritime Cross Sector Council for ports and terminals. He sits on the Safety and Security Division (SAFESEC) committee and is their liaison to the ISA Global Cybersecurity Alliance.

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.

Roy Smith
President
Viking Tactical Security Group

Roy Smith is currently the President of the Viking Tactical Security Group. He is an owner-operator. He is a certified Executive Protection Specialist with a proven employment record as a Law Enforcement Professional. He has worked for County, State, and Federal Agencies as a Law Enforcement Officer. Roy holds a Master’s Degree in Criminal Justice Administration with an emphasis in Emergency Preparedness and Risk Assessments. As President, Roy is the Operational Manager over the Executive Protection Division within Viking Tactical Security Group. One of his main duties is to evaluate each client’s needs, risks and assess the vulnerabilities and provide recommendations. Roy is also certified in Gangs, Cartels, and Terrorist organizations, as well as Active Shooter Situations. Roy is also one of the trainers for the Executive Protection Division within Viking Tactical Security Group.
Frederic Petit  
Principal Infrastructure Analysis  
Argonne National Laboratory

Frédéric Petit is a Research Scientist specializing in critical infrastructure interdependencies and resilience at Argonne National Laboratory. With a background in earth sciences and civil engineering, Dr. Petit has focused on risk management, business continuity, and infrastructure resilience since 2002. Frédéric leads the development of methodologies for the assessment of preparedness, mitigation, response, recovery, and overall resilience capabilities of facilities, communities, and regions. Dr. Petit is an internationally recognized expert in the area of infrastructure interdependency, and is the co-author of the standard operating procedure used by government agencies to better understand and incorporate these complex relationships into their assessment programs. Dr. Petit received his PhD from the École Polytechnique de Montreal in Civil Engineering, focusing on vulnerability analysis techniques for critical infrastructure cyber dependencies. Dr. Petit also serves as Regional Director for North America of the International Association of Critical Infrastructure Protection Professionals (IACIPP).

Ben Eazzetta  
CEO  
ARES Security Corporation

Ben Eazzetta is currently the CEO of ARES Security Corporation, interim CEO of Confluence Security Group, and a sitting board member for numerous private companies. Mr. Eazzetta was previously President of International Operations for Rolta India Limited, a leading multinational technology services provider serving North America, Asia/Pacific, Europe, and the Middle East, growing the International business from $25M of annual revenue to over $300M over 5 years. Ben joined Rolta after having served as president of Intergraph’s Security, Government, and Infrastructure division, where he was responsible for all aspects of global sales, marketing, delivery, and business development. Before Intergraph, Ben was the vice president and co-founder of Industria.com and beforehand worked at Exxon Company, USA, for more than twelve years, where he began his career as a mechanical engineer and was promoted ultimately to lead the operations and maintenance departments responsible for safety, operations, training, and contract administration.

Lawrence Paul Lewis  
Program Lead, Decision and Infrastructure Sciences Division  
Argonne National Laboratory

Lawrence “Paul” Lewis is the Program Lead for Technology Implementation in the Decision and Infrastructure Sciences Division. In this capacity, Paul leads multidisciplinary analyses of critical infrastructure protection and community resilience strategies across the country, and the development of decision support tools to address these challenges. Paul’s primary project is support of the U.S. Department of Homeland Security Office of Infrastructure Protection’s Regional Resiliency Assessment Program (RRAP), which seeks to identify single points of system failure, opportunities for closing gaps in coordinated preparedness, and address potential consequences of cascading impacts to interdependent social and physical infrastructure.

In addition, Paul has developed decision support tools for international humanitarian assistance programs for the U.S. Department of Defense, energy supply chain security programs for the U.S. Department of Energy, and served as lead social scientist in the development of community resiliency frameworks for Argonne’s Center for Integrated Resiliency Analysis. Paul is also a Lecturer in the Threat and Response Management program at the University of Chicago, where he teaches a course on emergency management policymaking, law, and ethics. Paul received his B.A. and M.A. from Tulane University in New Orleans, his J.D. from Tulane University Law School, and his M.S. from the University of Chicago.
Timothy Klett  
Cybersecurity Researcher  
Idaho National Laboratory

Tim Klett is a Cyber Security Researcher within the Infrastructure Assurance and Analysis Division at the Idaho National Laboratory (INL). He has over 18 years of experience in working with technology solutions for both the Department of Energy (DOE) and the Department of Homeland Security (DHS). His current work includes leading a DHS regional assessment to improve the understanding and management of vulnerabilities of water infrastructure to cyber threats among Federal, State, local, and private sector partners. Tim’s current research areas include cyber/physical impacts and critical infrastructure dependencies and interdependencies. Tim is currently pursuing a PhD in Computer Science from the University of Idaho, earned his M.S. degree in Computer Science from the Illinois Institute of Technology in 2004, and is a Certified Information Systems Security Professional (CISSP).

Steve Povolny  
Head of Advanced Threat Research  
McAfee

Steve Povolny is the Head of McAfee Advanced Threat Research, which delivers groundbreaking vulnerability research spanning nearly every industry. With more than a decade of experience in network security, Steve is a recognized authority on hardware and software vulnerabilities, who regularly collaborates with influencers in academia, government, law enforcement, consumers and enterprise businesses of all sizes. Steve is a sought-after public speaker and media commentator who often blogs on key topics. He brings to McAfee his passion for threat research and a unique vision to harness the power of collaboration between the research community and product vendors, through responsible disclosure, for the benefit of all.

Ruth Christensen  
Counterterrorism Analyst, National Counterterrorism Center, USA

Ruth Christensen serves as a counterterrorism analyst on NCTC’s Energy Cell. NCTC leads and integrates the national counterterrorism effort by fusing foreign and domestic CT information, providing terrorism analysis, and sharing information with partners across the CT enterprise. The Energy Cell focuses on non-state actor’s ability to target energy infrastructure. Prior to working at NCTC, Ruth served as an Intelligence Specialist in the US Navy from 2004-2012 and as an imagery analyst at the National Geospatial Intelligence Agency from 2012-2018.

Full speaker lineup at [www.ciprna-expo.com/speakers](http://www.ciprna-expo.com/speakers)

**REGISTER ONLINE AT WWW.CIPRMA-EXPO.COM**

Register Online Today at [www.ciprna-expo.com/onlinereg](http://www.ciprna-expo.com/onlinereg)
Organizations Participating Included:
The Venue and Accommodation

Doubletree by Hilton New Orleans-Airport
Williams Blvd, Kenner 70062
New Orleans
Louisiana

Double Tree by Hilton New Orleans Airport is just 10 minutes from Louis Armstrong New Orleans International Airport, with a free 24-hour shuttle both ways.

Every stay starts with a warm chocolate chip cookie, and our restaurant serves Creole-American dishes all day.

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

Accommodation

Special Room Rate for CIPRNA Delegates – $119 prpn incl breakfast (excl taxes)

Book your hotel accommodation at the Double Tree by Hilton New Orleans Airport at
www.ciprna-expo.com/hotel-booking

(Booking code: c21)

Delegates/attendees can make reservations in the following ways:

• Online: Reservations can be made online at www.ciprna-expo.com/hotel-booking using group code: c21

• Phone: Our Reservations Desk Direct at +1-504-4673111. Reference the group code: c21

We look forward to welcoming you to New Orleans
**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

---

**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 - $3,500
- Networking Reception Sponsor - $2,950
- Coffee Break Sponsor - $2,500
- Lanyard Sponsor - $1,950
- Badge Sponsor - $1,950

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 - $2,250**

7’ x 5’ 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 13.9% LOUISIANA/NEW ORLEANS SALES TAX
Sponsors and Supporters:

We wish to thank the following organisations for their support and contribution to Critical Infrastructure Protection & Resilience North America 2022.

Platinum Sponsor: 

Silver Sponsors:

Bronze Sponsors: 

Lanyard Sponsor: 

Coffee Break Sponsor:

Badge Sponsor:  

Flagship Media Partners:

Supporting Organisations:

Media Supporters:

Owned & Organised by:
DELEGATE REGISTRATION FORM

EARLY BIRD SAVINGS
Book your delegate place by 15th January 2022 and save with the Early Bird rate

REGISTRATION IS SIMPLE
1. Register online at www.cipma-expo.com/lonereg
2. Complete this form and email to: cipma@torchmarketing.co.uk
3. Complete this form and fax to +44 (0) 872 111 3210
4. Complete this form and mail to: CIPRE 2021, 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: ___________________________
Country: ___________________________
Post/Zip Code: ___________________________
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 1st February 2021.
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 30th September 2021. 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.
Alternations: 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 15th January 2022 ........................................... $195
Paid on or after 15th January 2022 ........................................... $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 15th January 2022 ........................................... $195
Paid on or after 15th January 2022 ........................................... $295

COMMERCIAL ORGANISATIONS
Individual Full Conference
(includes 3 day conference, conference proceedings, keynote, exhibition, networking reception, coffee breaks and lunch)
Paid before 15th January 2022 ........................................... $650
Paid on or after 15th January 2022 ........................................... $850

Individual Day Delegate
(includes access to conference on the day, coffee breaks and lunch on the day)
Paid before 15th January 2022 ........................................... $350
Paid on or after 15th January 2022 ........................................... $500
Attending on: [ ] 1st Feb  [ ] 2nd Feb  [ ] 3rd Feb

Exhibitor Full Conference
(includes 3 day conference, conference proceedings, keynote, exhibition, networking reception, coffee breaks and lunch)
Paid before 15th January 2022 ........................................... $325
Paid on or after 15th January 2022 ........................................... $425

Student Full Conference
(includes 3 day conference, conference proceedings, keynote, exhibition, networking reception, coffee breaks and lunch) - Student ID required
Paid before 15th January 2022 ........................................... $100
Paid on or after 15th January 2022 ........................................... $250

Conference Proceedings only ........................................... $495
EXHIBITION ONLY ........................................................... FREE
(includes access to exhibition floor only)

PAYMENT DETAILS
(METHOD OF PAYMENT - Conference fees include Louisiana Sales Tax at 13.9%.)
[ ] Wire Transfer (Wire information will be provided on invoice)
[ ] Credit Card
Involved 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 cipma@torchmarketing.co.uk