critical infrastructure PROTECTION AND RESILIENCE AMERICAS

December 5-7, 2017

Kennedy Space Center, Florida

www.ciprna-expo.com

Collaborating and Cooperating for Greater Security

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.

REGISTER TODAY
Early Bird Discount
deadline
November 5th,2017

Earn CEUs
Certified Training Workshop
details inside

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.

SPECIAL GOVERNMENT DEAL
Register by Nov 5th
see inside for details

Leading the debate for securing America's critical infrastructure

Platinum Sponsor: BLUVECTOR

Gold Sponsor: Belcan

Chief DISA/DoDIN Critical Infrastructure Protection (CIP) Program

Supporting Organisations:

Media Partners: World Security-Index.com, WORLD SECURITY REPORT

Welcome to 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 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 need 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 Kennedy Space Center's Center for Space Exploration on December 5th-7th, 2017.

Follow us:

Why Attend?

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

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

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

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

For conference or registration queries please contact:
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/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 at the Kennedy Space Center, Florida 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 December 5th, 2017

2:00pm-3:30pm - Opening Keynote Session
3:30pm-4:00pm - Networking Coffee Break
4.00pm-5:30pm - Plenary Session 1: Developing Greater Resilience in CNI
7:00pm - Welcome Reception

Wednesday December 6th, 2017

9:00am-10:30am - Plenary Session 2: FEMA: Long Term Power Failure Workshop
10:30am-11:15am - Networking Coffee Break in Exhibition Hall
11.15am-12:30pm - FEMA: Long Term Power Failure Workshop
12:30pm-2:00pm - Delegate Networking Lunch

Critical Infrastructure Protection Track

2:00pm-3:15pm - Session 3a: Emerging Threats on CNI
3:15pm-4:00pm - Networking Coffee Break
4:00pm - 5:30pm - Session 4a: Standards and Best Practice in CIP and Resilience

Critical Information Infrastructure Protection / Cyber Security Track

2:00pm-3:15pm - Session 3b: Cyber Security Legislation, Best Practice & Standards
3:15pm-4:00pm - Networking Coffee Break
4:00pm - 5:30pm - Session 4b: Cybersecurity Threats and Trends

5:30pm - Networking Reception in Exhibition Hall

Thursday December 7th, 2017

Critical Infrastructure Protection Track

9:00am-10:15am - Session 5a: Enhancing Preparedness and Response Capabilities
10:15am-11:00am - Networking Coffee Break
11:00am - 12:30pm - Session 6a: Technologies to Detect and Protect

Critical Information Infrastructure Protection / Cyber Security Track

9:00am-10:15am - Session 5b: Cyber Defence Strategies for CII
10:15am-11:00am - Networking Coffee Break
11:00am - 12:30pm - Session 6b: Operationalizing Resilience

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

2pm-2:45pm - Plenary Session 7: PPP & Collaboration in CIP and CIIP

2:45pm-3:30pm - Plenary Session 8: Critical Infrastructure Interdependencies

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

Exhibition Opening Hours		On-Site Registration Hours	
Tuesday December 5th	1.00pm to 5.00pm	Tuesday December 5th	8.00am to 5.00pm
Wednesday December 6th	9.30am to 7.00pm	Wednesday December 6th	8.30am to 7.00pm
Thursday December 7th	9.30am to 4.30pm	Thursday December 7th	8.30am to 4.00pm

REGISTER ONLINE AT WWW.CIPRNA-EXPO.COM

AGENCY REGISTRATION
Register Online at
www.ciprna-expo.com/agency-reg

ALL OTHER REGISTRATIONS
Register Online at
www.ciprna-expo.com/onlinereg

REGISTRATION
The Critical Infrastructure Protection & Resilience North America is open 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. Applications will be reviewed and considered on an individual basis. Delegates are requested to register sufficiently early to ensure participation. For all above mentioned communities the Critical Infrastructure Protection & Resilience North America early registration is "**Free of Charge**" for registration prior to November 5th.
REGISTER ONLINE TODAY AT WWW.CIPRNA-EXPO.COM/AGENCY-REG

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

EARLY BIRD DISCOUNT - deadline November 5th,2017
Register yourself and your colleagues as conference delegates by November 5th, 2017 and save with the Early Bird Discount.
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 rate:

- National Security & Resilience Consortium (NS&RC)
- International Association of CIP Professionals (IACIPP)
- International Security Industry Organization (ISIO)
- Association of Risk and Crisis Communication (ARCC)
- Security Partners Forum (SPF)
- Global Institute for CyberSecurity & Research (GICSR)

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

Tuesday December 5th

Conference Programme

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

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

Fred Ruonavar
Chief of DISA/DODIN Critical Infrastructure Program

Bryan Koon
Director, Florida Division of Emergency Management

Senior Representative, Department of Homeland Security

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

4:00pm-5:30pm - Plenary Session 1: Developing Greater Resilience in CNI

Hurricanes, Tornado's and Flooding are a certainty, the only uncertainty is exactly where and when. Cyber security attacks can also now be added to the list of certainties, as they are now a daily occurrence. Man-made disasters and large scale terrorist attacks on CNI are deemed likely, so building resilience into our systems and services is crucial if we are to mitigate the impact on our security, economy, national public health and safety..

Chair: Frederic Petit, Regional Director, International Association of CIP Professionals

Protected Critical Infrastructure Information (PCII) Program
Senior Representative, Office of Infrastructure Protection, U.S. Department of Homeland Security

Senior Representative, Public Safety Canada*

Senior Representative, DHS Office of Infrastructure Protection Programs

Senior Representative, Protective Security Coordination Division, Dept of Homeland Security

Michael Lowder
Director - Office of Intelligence, Security & Emergency Response, US Dept of Transportation

---

7:00pm-9:00pm - Welcome Reception (tbc)

**invited*











Wednesday December 6th

9:00am-10:30am - Session 2: FEMA Workshop

Chair: David Fortino, Regional Continuity Manager,Federal Emergency Management Agency (FEMA)

Long Term Power Failure Workshop

The focus of this workshop is specifically the local level response and interaction / coordination of local and state agencies and private sector partnerships.

The workshop will yield a better understanding of how LTPO response is managed and its relationship within the multi-agency coordination concept.

The discussion will assist in improving sustainment of power and response continuity.

Private sector, state and local government entities will have the opportunity to participate in discussions addressing an LTPO.

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

11:15am-12:30pm - FEMA Workshop (pt 2)

Continuing the Long Term Power Failure Workshop hosted by FEMA

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




Wednesday December 6th

Critical Infrastructure Protection Track

2:00pm-3:15pm - Session 3a: Emerging Threats on CNI

Threats to critical national infrastructure come in many forms, whether it is UAV's, disruption of GPS/ GNSS signals or flood waters. Identifying new and potential threats is crucial to enabling governments, law enforcement, operators and stakeholders to take the necessary steps to mitigate against possible disruption.

Chief of the Operations Division and Director of the NWS Operations Center*

Senior Representative, U.S. Southern Command (SOUTHCOM)*

Securing GNSS for Critical Infrastructure
Guy Buesnel, PNT Security Technologist, Spirent Communications

The Insider Threat
Sarah-Jane Prew, Crime Stoppers UK

3:15pm-4:00pm - Networking Coffee Break

4:00pm - 5:30pm - Session 4a: Standards and Best Practice in CIP and Resilience

Protection and resilience of CNI can be driven by minimum standards and best practice, but how are these developed and met? What is considered a minimum standard and how can standardizations of standards and best practice meet the challenge?

Robert Crane, Advisor National Coordination Office for Space-Based Positioning, Navigation and Timing, DHS

Senior Representative, Orlando Airport*

Michelle Deane, Director, Homeland Defense and Security Standardization Collaborative (HDSSC), American National Standards Institute's Homeland Security Standards Panel (ANSI-HSSP)

Keeping the Lights on: Protecting America's Electric Grid from Attack
Brian Harrell, Vice President of Security, AlertEnterprise

Critical Information Infrastructure Protection / Cyber Security Track

2:00pm-3:15pm - Session 3b: Cyber Security Legislation, Best Practice & Standards

As cyber-attacks become increasingly common, it is the role state actors to ensure that robust and comprehensive legislation is in place to ensure the proper protection and resilience of critical national infrastructure as well as promote the application of best practice.

Chair: Deborah Kobza, President/CEO, The Global Institute for Cybersecurity + Research

Mike Echols, CEO, ISAO

Is Privacy at Odds with the Information Sharing Environment?
James Emerson, Chairman of the Computer Crime and Digital Evidence Committee, International Association of Chiefs of Police

Michael Daniel, President, Cyber Threat Alliance

3:15pm-4:00pm - Networking Coffee Break

4:00pm - 5:30pm - Session 4b: Cybersecurity Threats and Trends

The digital age has opened up immense new opportunities for criminal activity, providing numerous communications channels and instant access to critical information and data. But what are the latest threats in the cybersecurity space and what are the future trends likely to be in attacks on our critical information infrastructure.

Mark Dubina, Director of Security, Tampa Port Authority

Critical Infrastructure Protection: Beyond the Hybrid Port and Airport Firmware Security
Andrea Chiappetta, Professor of Geopolitics, Marconi International University

Michael Baisden, Cyber Security Solutions Manager, Belcan

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

Thursday December 7th

Critical Infrastructure Protection Track

9:00am-10:30am - Session 5a: Enhancing Preparedness and Response Capabilities

Prior, planning and preparation is the key to ensuring that CNI operators have the right equipment, processes and procedures in place to respond in the event of an emergency.

Policy and technical support to the EPCIP and the fight against Terrorism
Alessandro Lazari, Contract Agent, European Commission – Joint Research Centre – Directorate "Space, Security and Migration" – Unit E.02 "Technology innovation in Security"

Carlos Morales, Manager of Critical Infrastructure & Compliance, NextEra Energy / Florida Light & Power

Assistant Director Division of Emergency Management, State Department of Texas*

Director, California Governor's Office of Emergency Services*

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

11:15am - 12:30pm - Session 6a: Technologies to Detect and Protect

What are some of the latest and future technologies, from ground surveillance to space based technology, to predict or detect potential threats to CNI, whether natural or terrorist related..

Matt Conner, Chief Information Security Officer, National Geo-Spacial Intelligence Agency

Effective & Efficient Perimeters - Radar Video Surveillance
Adrian Fielding, Global Marketing Director - Integrated Protective Solutions, Honeywell Performance Materials & Technologies

Chemical Threat Early detection for Critical Infrastructures
Sebastien Blanchard, Sales Manager, Bertin Corp

Drone Security: State of an Evolving Threat
Andrew Tormey, Business Development, Gryphon Sensors

Critical Information Infrastructure Protection / Cyber Security Track

9:00am-10:30am - Session 5b: Cyber Defence Strategies for CII

How do we ensure that CNI operators have the right analysis and protection systems in place to prevent the disruption or destruction critical information infrastructure (CII) and have the right resilience proceedures in place the event of a breach.

Gulf of Mexico Maritime Cyber Workshop review
Christy Coffey, Maritime & Port ISAO

Mitigating Risks in the Innovation Economy
Victoria Sherazi, Project Lead "Mitigating Risks in the Innovation Economy", World Economic Forum

International Focus on Regional Resilience
Stacey Stanchfield, Lead Cybersecurity Engineer, MITRE

Multiple OS Rotational Environment Moving Target Defense as a Proactive Defense against Zero-Day Vulnerabilities
Nathaniel Evans, Cyber Operations, Analysis and Research Lead, Argonne National Laboratory

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

11:15am - 12:30pm - Session 6b: Operationalizing Resilience

In view of realities and what practitioners know "keep them awake at night," this session will discuss the relationship between "information sharing", intelligence gathering and target identification and assessment in IOT and present proven and actionable solutions to operationalize resilience and correct a critical infrastructure, business, community and National preparedness situation, that in the absence of resilience will continue to deteriorate..

Chair: Judge William H. Webster, the Chairman of the Homeland Security Advisory Council (HSAC)

Kathy Francis, Executive Director of Emergency Management Mid, Atlantic Center for Emergency Management, Frederick Community College, Maryland

Jeff Gaynor, President, American Resilience

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

Thursday December 7th

2pm-3:00pm - Plenary Session 7: PPP & Collaboration in CIP and CIIP

As so much critical national infrastructure is in the hands of public sector organizations - Public Private Partnership is a prerequisite for successful risk management and resilience.

Chair: John Donlon QPM FSI

Judge William H. Webster, the Chairman of the Homeland Security Advisory Council (HSAC)

Global Mission Assurance Program (GMAP): Establishing Integrated Situational Awareness via Streamlined Data Sharing for Collection and Visualization
Joseph Wassel, Director, C4 Resilience & Mission Assurance, US Department of Defence

3pm-4:00pm - Plenary Session 8: Critical Infrastructure Interdependencies

It is the interdependencies between large numbers of independent critical national infrastructures that is the catalyst for multiple failures in the so called cascade effect. How do we identify the weaknesses and prevent and/or mitigate the effects?

Chair: John Donlon QPM FSI

William McNamara, DHS Office of Infrastructure Protection – Protective Security Coordination Division (PSCD)*

Going further than Physical and Cyber Connections: Consideration of Logical Interdependencies
Frederic Petit, Research Scientist, Argonne National Laboratory

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

Highlighted Speakers

Fred P. Ruonavar
Chief, DISA/DoDIN Critical Infrastructure Protection (CIP) Program
Defense Information Systems Agency, USA

Mr. Fred Ruonavar is the Chief of the Contingency Operations and DoD Information Network (DoDIN) Critical Infrastructure Protection (CIP) Branch in the Operations Directorate at the Defense Information Systems Agency (DISA), located at Fort George G. Meade, Maryland. He acts as the lead government agent for the DoDIN Sector CIP program. He serves as the technical advisor on matters involving infrastructure programs and organizational structures; evaluating directorate level plans and policies for use by Department of Defense employees in the development of information technology criteria; and Information Assurance programs and plans. In addition, he is the lead for the Agency's Combat Support feasibility planning, providing managerial and supervisory oversight to the DISA supplemental requirements in support of Operations Enduring Freedom, Iraqi Freedom, and other contingency operations in the Global War on Terrorism. Mr. Ruonavar also directs DoDIN/DISA CIP participation in annual COCOM Tier 1-level exercises, spearheading initiatives to implement standards, methodologies, and strategies that ensure the agency's mission of providing world class service to the warfighter.

While directing contingency operations as the Chief of the DISA Crisis Action Team (CAT), he received the prestigious Director's Award. Under his leadership DISA's CAT responded to numerous catastrophic events including multiple hurricanes, Mediterranean cable cuts, the Haitian earthquake, and the Tsunami Fukushima.

Prior to his civil service assignments, he was a Design Engineer for SAIC supporting Boeing Information Services. He maintained operations and analysis oversight for the Defense Information System Network (DISN) and Asynchronous Transfer Mode (ATM) networks, which served well over 10,000 customers.

Brian Koon
Director
Florida Division of Emergency Management

Bryan Koon has served as the Director of the Florida Division of Emergency Management since February, 2011. Prior to joining the Division, he worked with Wal-Mart Stores, Inc for five years as Operations Manager and Director of Emergency Management.

Bryan's experience within emergency management includes the private sector, federal government, and state government. Bryan worked at the White House Military Office for seven years where he was a Watch Officer in the President's Emergency Operations Center while on active duty with the U.S. Navy. He then spent two years as Training Officer for Presidential Contingency Programs, conducting training and exercises for the White House Military Office, United States Secret Service, Federal Emergency Management Agency, and others. After concluding his active duty Navy service, Bryan continued to serve at the White House as a contractor from SRA, International.

Bryan's specialty in the Navy was as a surface warfare officer. He served on two ships, USS INDEPENDENCE (CV 62) and USS PORT ROYAL (CG 73), where he made several deployments while serving as Main Machinery Room Officer and Main Propulsion Assistant.

Bryan is currently serving as the Vice Chairman of the Multi-Hazard Mitigation Council and is on the Board of Directors of the National Information Sharing Consortium. He is a past-president of the National Emergency Management Association (NEMA).

Michael W. Lowder
Director
Office of Intelligence, Security & Emergency Response, U.S. Department of Transportation, USA

Michael W. Lowder serves as the Director of the Office of Intelligence, Security & Emergency Response (S-60) for the U.S. Department of Transportation. A member of the Senior Executive Service (SES) and is designated as a National Security Professional and a Federal Senior Intelligence Coordinator. Mr. Lowder is the Department's Emergency Coordinator providing leadership for all departmental civil transportation intelligence issues, security policy, and emergency preparedness, response, and recovery activities related to emergencies that affect the viability of the transportation sector. In 2012 he was awarded the DOT Secretary's Gold Medal for Outstanding Achievement. He was selected in 2015 to represent the U.S. at the China Executive Leadership Academy (CELAP).

Prior to this Mr. Lowder served as the Deputy Director of the Response Division for the Federal Emergency Management Agency (FEMA) in Washington, D.C. Mr. Lowder has been designated and served as both a Principal Federal Official (PFO) and a Federal Coordinating Officer (FCO). Mr. Lowder was a member of FEMA's National Emergency Response Team (ERT-N), and a Domestic Emergency Response Team (DEST).

Mr. Lowder has more than 35 years of experience in the law enforcement, and emergency services field, as a Special Agent with the US Government, the State of North Carolina as a Special Agent with the North Carolina State Bureau of Investigation, and as the Director of Emergency Services with Bladen County, North Carolina.

Mr. Lowder has represented the U.S. government at meeting and conferences in the United Kingdom, Russia, China, Australia, Japan, Belgium, Taiwan, and Turkey, as well as throughout the United States. He represented the U.S. at NATO-RUSSIA counter-terrorism exercises in Kaliningrad, Russia and the 'Black Rain' CT exercises in the UK. He serves on the Executive Board on the FBI's National Joint Terrorism Task Force (NJTTF), the ODNI's National HUMINT Committee, and represents the Department on National Security Council (NSC) and Homeland Security Council (HSC) policy and advisory groups. He is the US lead for the US-China Transportation Forum - Transportation Emergencies Working Group. He also serves as the DOT lead on the US-Russia Joint Committee on Cooperation in Emergency Management.

Joseph M. Wassel
Director, C4 Resilience & Mission Assurance
US Department of Defense, USA

Joseph M. Wassel is the Director of C4 Resilience & Mission Assurance in the Department of Defense (DoD) Chief Information Officer's (CIO's) office. He is responsible for overseeing the development of an Enterprise Environment that informs risk management decisions across all the functional areas of mission assurance. His portfolio within DoD CIO focuses on combining critical infrastructure knowledge management, intelligence, and alerts to enable analytic views of critical infrastructure, DoD vulnerability assessments, dependency analysis, and threat reporting. He strives to continuously improve the resilience of the nation's critical assets by sharing information and collaborating across military and non-military partners.

Mr. Wassel is also the Chair of the DoD Public Safety Communications Working Group. In this capacity, he leads the Services, Joint Staff, National Guard, NORTHCOM and other DoD partner activities for the Department's public safety communications efforts to include FirstNet planning and implementation, 911 services and Defense Support to Civil Authorities (DSCA) communications. Additionally, he is the Program Director for the Global Mission Assurance Portal and is responsible for developing classified portals which provide senior leaders with critical infrastructure decision support through dynamic geospatial visualization.

Prior to assuming his current positions, Mr. Wassel was the Assistant to the Secretary of Defense for Communications and Deputy Chief Information Officer for OSD. In that capacity, he served four Secretaries of Defense (Perry, Cohen, Rumsfeld, and Gates) as the Secretary's principal liaison and single focal point to all agencies providing the required global communications support. He was responsible for connecting and informing the SecDef during every major crisis the Department and the Nation faced for over a decade. During his tenure, he traveled worldwide on Secretary of Defense travel missions to over 100 countries, logging over 900 days deployed and several thousands of hours as the Senior Communications Official on the National Airborne Operations Center, E4-B, and other VIP aircrafts supporting the Secretaries of Defense.

Nathaniel Evans
Cyber Operations, Analysis and Research Lead
Argonne National Laboratory

Dr. Nate Evans currently serves as the lead for the Cyber Operations, Analysis and Research group at Argonne National Laboratory. Nate received his Doctorate in Computer Engineering with a specialty in Cybersecurity from Iowa State University. Prior to joining Argonne, Nate managed cybersecurity and cyber defense activities at several private-sector companies. He is considered a key asset by the Department of Homeland Security (DHS) in several cybersecurity capabilities including the development of a cybersecurity vulnerability assessment for field use, analysis of cybersecurity consequence and threat studies, and leading the pilot cyber-physical regional assessment. Nate has also developed a patent pending operational instance of moving target defense (MTD) and has worked in a variety of other cybersecurity research areas including transportation, satellite communications, social engineering, and offensive cybersecurity. He has taught computer networking and cybersecurity issues to students in Senegal, Africa, through the African Institute for Mathematical Sciences (AIMS) Next Einstein Initiative, a collaboration with the University of Chicago, Argonne and other institutions. He also led the development of Argonne's Collegiate Cyber Defense Competition, drawing college students from across the Nation, in the defense of realistic attacks on simulated critical infrastructure.

Adrian Fielding
Business Leader – Telecoms & Security Integration
Honeywell Performance Materials & Technologies

Adrian Fielding is the Business Leader for Telecoms & Security Integration (TSI) and works on Honeywell Process Solutions' global marketing team. He has been part of the Global Industrial Security initiative with Honeywell for more than 11 years. As well as leading the TSI consulting team, Adrian is responsible for the coordination of Honeywell's strategic partners, business development and product marketing of key solutions for the protection of large- and medium-sized operations. This includes, but is not limited to: refineries, pipelines, power plants, chemical plants, on- and off-shore facilities, and industrial ports.

Adrian has a strong technical background, which he acquired from 10 years of service as an Avionics Engineer with the Royal Air Force.

David Fortino, Regional Continuity Manager, Federal Emergency Management Agency (FEMA), USA

James Emerson, Chairman of the Computer Crime and Digital Evidence Committee, International Association of Chiefs of Police

Sarah-Jane Prew, Crime Stoppers UK

Brian Harrell, Vice President of Security, AlertEnterprise

Sebastien Blanchard, Sales Manager, Bertin Corp

Networking Reception

Wednesday December 6th
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.

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.

Built in security - increasing security without turning our public buildings and spaces into fortresses

The Venue

Center for Space Education
Kennedy Space Center Visitors Center
NASA's Kennedy Space Center
Cape Canaveral
Florida, FL 32899

After five decades, NASA's John F. Kennedy Space Center continues to lead America's adventure into space and is an integral part of the country's national infrastructure and security programs.

As the Kennedy Space Center is transforming to a multiuser spaceport to support both government and commercial customers, the center is looking toward the future as a dynamic infrastructure takes shape, designed to host many kinds of spacecraft and rockets sending people, satellites and equipment into space.

NASA's Ground Systems Development and Operations Program will provide 21st century ground systems for processing and launch. NASA's Launch Services Program (LSP) will continue to procure Expendable Launch Vehicles to enable satellites and robotic missions on their journey to learn more about our home planet and unlock the secrets of the universe.

Kennedy will continue to support International Space Station operations as the orbiting laboratory enters its second decade of discoveries. Kennedy is spearheading the way to return NASA astronauts to low-Earth orbit in safe, reliable and affordable space transportation systems through NASA's Commercial Crew Program (CCP).

The Ground Systems Development and Operations (GSDO) Program was implemented at Kennedy to modernize its facilities for multiple commercial and

government customers. The goal of the GSDO Program is to transform the Florida launch and range complex by implementing a focused set of investments to its infrastructure, creating a multiuse spaceport of choice for NASA and other users. The program aligns with the needs of civil, national security, and commercial enterprises, ultimately extending to the international space community.

NASA's Kennedy Space Center remains a very significant economic driver and a major contributor to the economic health of the state of Florida. Analysis of the Fiscal Year 2012 expenditures concludes that overall NASA activities and ones specifically related to Kennedy across Florida contribute about $1.3 billion in wages and purchases to the state economy.

The Kennedy Space Center is the ideal location to host the inaugural **Critical Infrastructure Protection & Resilience North America** and look at the challenges and issues faced in todays world of heightened situational threats.

www.kennedyspacecenter.com

Accommodation

Event HQ Hotel

Holiday Inn Titusville
4715 Helen Hauser Blvd, Titusville
FL 32780, USA
T: +1 321-383-0200

Special Room Rate for CIPRNA Delegates - $109 prpn incl breakfast (excl taxes)

Titusville Hotel's Location is Near the Kennedy Space Center.

The 3 star Holiday Inn® Titusville - Kennedy Space Center hotel is one of the most recent additions to Titusville, FL. The hotel's convenient location and amenities make it a perfect choice for your visit to the Kennedy Space Center and your stay for the CIPRNA event.

Business travelers appreciate being close to major corporations in the area. Complimentary high-speed, wireless Internet access and two meeting rooms make this hotel a convenient choice.

The hotel's guests in Titusville, FL enjoy top-notch amenities, an outdoor, heated pool and a 24-hour Fitness Center. Our restaurant, Bapa's Bistro & Lounge, is open for breakfast and dinner, serving casual American cuisine in a relaxed and welcoming atmosphere.

The Holiday Inn Titusville is offering delegates to CIPRNA a special rate of $109 prpn including breakfast (excl. taxes).

Book your hotel accommodation directly using the special link to obtain your preferential rate:

www.ciprna-expo.com/holiday-inn

Group code: CIP

Alternate Hotel

Fairfield Inn & Suites Titusville Kennedy Space Center
4735 Helen Hauser Blvd, Titusville
FL 32780, USA
T: +1 321-385-1818

Special Room Rate for CIPRNA Delegates - $129 prpn incl breakfast (excl taxes)

The Fairfield Inn & Suites Titusville is the closest Marriott to the Kennedy Space Center, only 20 minutes north of Port Canaveral just off I-95.

The Fairfield Inn & Suites Titusville Kennedy Space Center offers complimentary Wi-Fi and hot breakfast buffet. The hotel offers a well-equipped 24-hour business center, exercise room, outdoor heated pool, 24-hour Market and rooms have mini-refrigerators and flat screen TVs. Fairfield Inn features rooms equipped with a hair dryer.

With numerous amenities this art deco hotel features include a BBQ/picnic area and vip rooms. This 3-star hotel provides a laundry service, an ice machine and off-site parking. Pets are also welcome.

The Fairfield Inn Marriott Titusville is offering delegates to CIPRNA a special rate of $129 prpn including breakfast (excl. taxes).

Book your hotel accommodation directly using the special link to obtain your preferential rate:

www.ciprna-expo.com/fairfield-inn

***Communications Resilience** – In the event of a disaster, how do you keep the information flowing*

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 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.

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:

Paul McPherson
(Americas)
E: paulm@torchmarketing.co.uk
T: +1-240-463-1700

Paul Gloc
(UK and Rest of Europe)
E: paulg@torchmarketing.co.uk
T: +44 (0) 7786 270 820

Marc Soeteman
(Benelux & Germany)
E: marcs@torchmarketing.co.uk
T: +31 (0) 6 1609 2153

Jerome Merite
(France)
E: j.callumerite@gmail.com
T: +33 (0) 6 11 27 10 53

Exhibiting Investment

The cost of exhibiting at the Critical Infrastructure Protection & Resilience Americas is:

Standard 10'x10' Booth, with pipe and drape - US$40 per sq.ft.
(EARLY BIRD: Contract completed and returned by 15th August 2017 - US$36 sq.ft.)

Standard Package includes: 10'x10' floor space, pipe and drape, 1 x table and 2 x chairs, 2 exhibition booth passes with lunch and coffee breaks included, listing in the official event guide and website.

Table Top Information Stand - $2,000
(EARLY BIRD: Contract completed and returned by 15th August 2017 - US$1,500)
7' x 5' raw space with 1 x table and 2 x chairs, 1 exhibition booth pass with lunch and coffee breaks included, listing in the official event guide and website.

Additional Exhibition Booth Passes can purchased at a cost of US$150 each, which includes lunch and coffee breaks for the two days.

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

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 on the left. Packages can be designed and tailored to meet your budget requirements and objectives.

Sponsors and Supporters:

We wish to thank the following organisations for their support and contribution to Critical Infrastructure Protection & Resilience North America 2017.

Platinum Sponsor:

BLUVECTOR™

Gold Sponsor:

Belcan

Supporting Organisations:

Chief of DISA/DODIN

International Association of CIP Professionals

NS&RC

ISIO

SPF

The Global Institute for Cybersecurity + Research

ASSOCIATION OF RISK AND CRISIS COMMUNICATION

Media Partners:

World Security-index.com

WORLD SECURITY REPORT

Owned & Organised by:

TORCH

K-N-M MEDIA

Media Supporters:

airport SUPPLIERS

AVIATION SECURITY INTERNATIONAL

defence SUPPLIERS

domestic preparedness .com

EH ECOURBANHUB

Global Security Mag THE LOGICAL & PHYSICAL SECURITY MAGAZINE

DIGITAL FORENSICS / MAGAZINE

EIN PRESSWIRE

CRITICAL INFRASTRUCTURE PROTECTION REVIEW