

critical infrastructure PROTECTION AND RESILIENCE AMERICAS

March 12th-14th, 2024
LAKE CHARLES, LOUISIANA
www.ciprna-expo.com

critical infrastructure PROTECTION AND RESILIENCE EUROPE

12th-14th November 2024
Madrid, Spain
www.cipre-expo.com

Collaborating and Cooperating for
Greater Security

Securing the Inter-Connected Society



Exhibitor Prospectus & Media Info

Critical Infrastructure Protection and Resilience events bring together leading stakeholders from industry, operators, agencies and governments to debate and collaborate on securing the nations critical infrastructure.

Gain access to leading decision makers from corporate and government establishments tasked with Critical Infrastructure Protection and Resilience.

Flagship Media Partner:

critical infrastructure
PROTECTION AND
RESILIENCE NEWS





Co-Hosted by:



Supported by:



Supporting Organisations:



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.

The Critical Infrastructure Protection and Resilience North America conference 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.

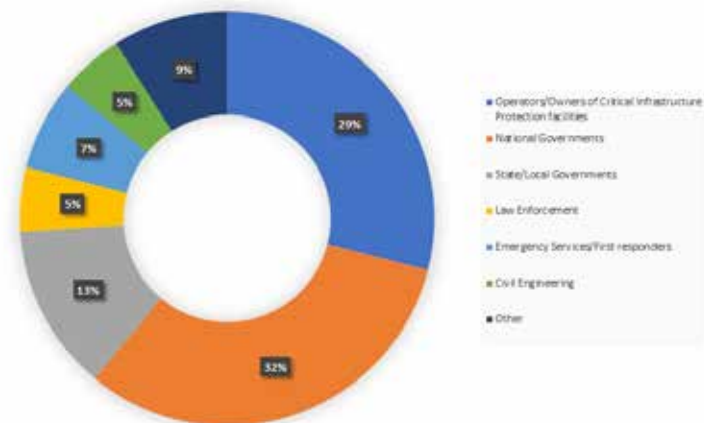
The ever changing nature of threats, whether natural through climate change, or man-made through terrorism activities, either physical or cyber-attacks, means the need to continually review and update policies, practices and technologies to meet these demands.

- | | |
|--|---|
| <ul style="list-style-type: none"> • <i>Chemical Sector</i> • <i>Commercial Facilities Sector</i> • <i>Communications Sector</i> • <i>Critical Manufacturing Sector</i> • <i>Dams Sector</i> • <i>Defense Industrial Base Sector</i> • <i>Emergency Services Sector</i> • <i>Energy Sector</i> | <ul style="list-style-type: none"> • <i>Financial Services Sector</i> • <i>Food and Agriculture Sector</i> • <i>Government Facilities Sector</i> • <i>Healthcare and Public Health Sector</i> • <i>Information Technology Sector</i> • <i>Nuclear Reactors, Materials, and Waste Sector</i> • <i>Transportation Systems Sector</i> • <i>Water and Wastewater Systems Sector</i> |
|--|---|

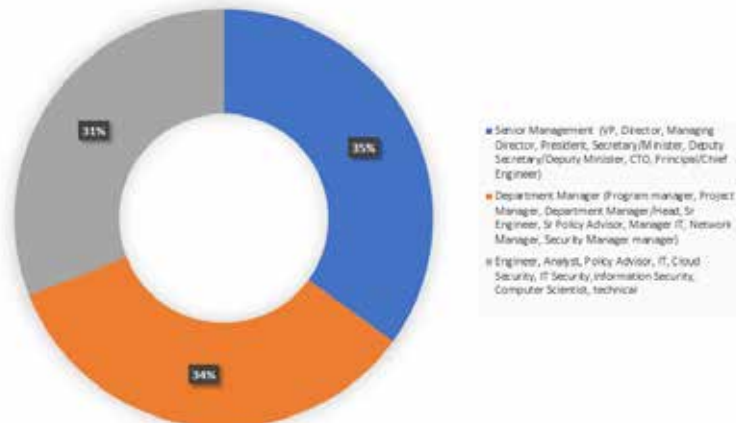


Statistics

Organization Type



Job Function



Over 300 Delegates

Over 300 delegates attended the conference and expo in 2023.

\$3.5 million

average amount of the budget size that the attendees are responsible for.

Key Partners

Key partner organizations, such as CISA, TSA, FBI, USCG, IACI and TIEMS participated in 2023

85.7%

of attendees are involved in their organizations purchasing process for Critical Infrastructure Protection products

Serious About Security

Delegates attended to learn and discover how to secure their assets from emerging threats

To find new solution providers

biggest reason people attended the event

Uniquely Positioned

CIPRNA is the only event with the agenda for Critical Infrastructure Protection and Resilience

100%

of the attendees said they would attend Critical Infrastructure Protection show again!





Critical Information Infrastructure Protection / Cyber Security

With the ever increasing threat from cyber attacks on critical infrastructure, the information and data stored and used by CNI systems and operators can be more crucial than the system itself. CIIP is becoming ever more important as part of the cyber security strategy of an organisation or CNI operator.

The Critical Infrastructure Protection & Resilience North America conference will give you the opportunity to demonstrate and showcase your leading technologies, products and services available to the industry.

As an exhibitor you can meet leading decision makers from corporate and government establishments tasked with Critical Infrastructure Protection and Resilience and safer cities.

Who is CIPRNA for?

Critical Infrastructure Protection and Resilience Americas is for government agencies, critical infrastructure owner/operators, state and local security/intelligence/law enforcement and industry, including:

- National government agencies responsible for national security and emergency/contingency planning (FEMA / DHS, etc)
- Police and Security Agencies
- Emergency Services, Emergency Managers and Operators
- Local Government
- Facilities Managers – Nuclear, Power, Oil and Gas, Chemicals, Telecommunications, Banking and Financial, ISP's, water supply
- IT, Cyber Security and Information Managers
- Port Security Managers
- Airport Security Managers
- Transport Security Managers
- Engineers, Architects, Constructors and Landscape Designers
- Public Administrators and Managers
- Public Health, Safety, and Healthcare Professionals
- Academic and Research Professionals
- Utility Providers (Energy, Communications, Water)
- Policy, Legal and Law Enforcement
- Urban Planners and County Commissioners
- Transportation Managers and Planners
- Facility, Data and IT Managers
- Supply Chain Logistic Managers and Operators
- Event Security Managers
- Architects / Civil Engineers
- NATO / Military / Border Officials

Who should Exhibit

Critical Infrastructure Protection and Resilience North America provide great business development opportunities, as well as connections to a key target audience, for:

- Security equipment manufacturers and suppliers
- IT security consultants
- Infrastructure protection consultants
- Architects
- Builders
- Civil Engineers
- Security Service providers

Benefits of Exhibiting

- Build and enhance your company profile and image to key industry professionals
- Connect with customers and develop new business relationships
- Showcase your products and services to key decision makers and buyers
- Communicate your company's news and messages direct to your potential customers
- Learn about the latest challenges and threats facing the critical infrastructure sector
- Connect with more customers in less time in the best face-to-face environment

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

For conference or registration queries please contact:

Ben Lane

Event Manager

T: +44 (0) 7956 899806

F: +44 (0) 872 111 3210

E: benl@torchmarketing.co.uk



Why participate and be involved?

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

Your participation will gain access to this key target audience:

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

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

www.ciprna-expo.com

How to Exhibit

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

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

Ray Beauchamp

Americas

E: rayb@torchmarketing.co.uk

T: +1 408-921-2932

Paul Gloc

Rest of World

E: paulg@torchmarketing.co.uk

T: +44 (0) 7786 270 820

Jina Lawrence

Rest of World

E: jinal@torchmarketing.co.uk

T: +44 (0) 7958 234750

Sam Most

Rest of World

E: samm@torchmarketing.co.uk

T: +44 (0) 208 123 7909

Sponsorship Opportunities

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

Some of the sponsorship package opportunities are highlighted here.

- Platinum Sponsor - \$14,950
- Gold Sponsor - \$10,500
- Silver Sponsor - \$8,950
- Bronze Sponsor - \$6,950
- Conference Proceedings Sponsor - \$4,950
- Site Visit & Coach Sponsorship - \$4,500
- Delegate Folder Sponsor - \$4,000
- Networking Reception Sponsor - \$3,500
- Coffee Break Sponsor - \$3,500
- Lanyard Sponsor - \$3,500
- Badge Sponsor - \$3,500

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

Please enquire for further details.

Exhibiting Investment

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

Table Top Exhibit 5'x7' - \$3,000

Table Top Exhibit 10'x10' - \$4,995

Raw space with 1 x table and 2 x chairs, pipe and drape, electrical socket, wi-fi, 1 Exhibitor Delegate pass (2 for 10x10) 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 additional Conference Delegate passes.

ASK ABOUT OUR BOOKING BUNDLES FOR EXTRA EXPOSURE

ALL PRICES SUBJECT TO 10.2% LOUISIANA/LAKE CHARLES SALES TAX



Supported by:

Lake Charles, Louisiana



Lake Charles (French: Lac Charles) is the fifth-largest incorporated city in the U.S. state of Louisiana, and the parish seat of Calcasieu Parish, located on Lake Charles, Prien Lake, and the Calcasieu River. Founded in 1861 in Calcasieu Parish, it is a major industrial, cultural, and educational center in the southwest region of the state.

The city and metropolitan area of Lake Charles is considered a regionally significant center of petrochemical refining, gambling, tourism, and education, being home to McNeese State University and SOWELA Technical Community College.

Strategically seated on the Calcasieu River in southwestern Louisiana, just 30 miles from the Gulf of Mexico, the Lake Charles area's assets are integral to the nation's logistics and energy networks.

Lake Charles has played a significant role in the growth and development of the state and now serves as an economic hub, with many major companies based in the area, and strategic point for critical infrastructure serving the south west. The Lake Charles area continues to be one of the fastest growing areas in the nation





critical infrastructure PROTECTION AND RESILIENCE EUROPE

12th-14th NOV 2024
Madrid, Spain
www.cipre-expo.com

Co-Hosted by:



Supporting Organisations:



CIPRE – Where CIIP/Cyber and Physical Security Meet

Attacks on critical infrastructure sites are now a fact of life not simply a potential threat. Power stations, chemical plants, nuclear facilities are routinely targeted by cyber-attacks, the most successful so far being the Ukraine power outage that caused 225,000 customers to lose electricity. Last year an activist landed a UAV carrying small traces of radiation on the roof of the Japanese Premier's office and this year a UAV collided with a aircraft at London's Heathrow airport. And of course the terrible attacks on the metro and airport in Brussels. This is just the start of what we can expect to be the repeated targeting of our critical infrastructure. The potential effects not only in terms of loss of life but also in terms of damage to infrastructure, economic disruption and costs, can be enormous.

We must be prepared!

The European Commission has adopted a communication on Critical Infrastructure Protection in the fight against terrorism, enhancing European prevention, preparedness and response in the event of terrorist attacks involving critical infrastructures.

The European Programme for Critical Infrastructure Protection (EPCIP) considers measures that will enhance the level of protection of infrastructure against external threats, with the Operator Security Plan for all infrastructures designated as European critical.

Learn about the importance of the updated NIS2 Directive...

An important discussion will centre around the EU cybersecurity rules introduced in 2016 and updated by the NIS2 Directive that came into force in 2023. It modernised the existing legal framework to keep up with increased digitisation and an evolving cybersecurity threat landscape. By expanding the scope of the cybersecurity rules to new sectors and entities, it further improves the resilience and incident response capacities of public and private entities, competent authorities and the EU as a whole.

Businesses identified by the Member States as operators of essential services in the above sectors will have to take appropriate security measures and notify relevant national authorities of serious incidents. Key digital service providers, such as search engines, cloud computing services and online marketplaces, will have to comply with the security and notification requirements under the Directive.

Learn about the importance of the new directive on the Resilience of Critical Entities...

The Directive on the Resilience of Critical Entities entered into force on 16 January 2023. Member States have until 17 October 2024 to adopt national legislation to transpose the Directive.

The Directive aims to strengthen the resilience of critical entities against a range of threats, including natural hazards, terrorist attacks, insider threats, or sabotage, as well as public health emergencies. Under the new rules:

- Member States will need to adopt a national strategy and carry out regular risk assessments to identify entities that are considered critical or vital for the society and the economy.
- In turn, the critical entities will need to carry out risk assessments of their own and take technical, security and organisational measures to enhance their resilience and notify incidents.
- Critical entities in the EU providing essential services in six or more Member States, will benefit from extra advice on how best to meet their obligations to assess risks and take resilience-enhancing measures.
- Member States will need to provide support to critical entities in enhancing their resilience. The Commission will provide complementary support to Member States and critical entities, by developing a Union-level overview of cross-border and cross-sectoral risks, best practices, guidance material, methodologies, cross-border training activities and exercises to test the resilience of critical entities, among others.



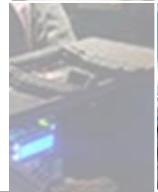
critical infrastructure PROTECTION AND RESILIENCE EUROPE



12th-14th NOV 2024

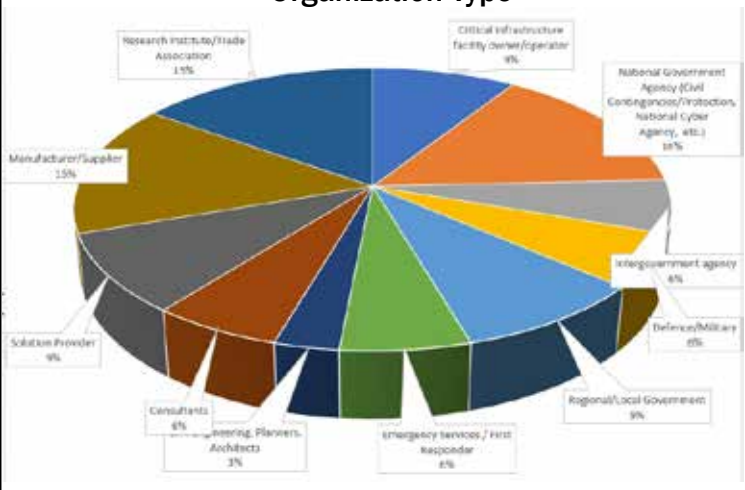
Madrid, Spain

www.cipre-expo.com

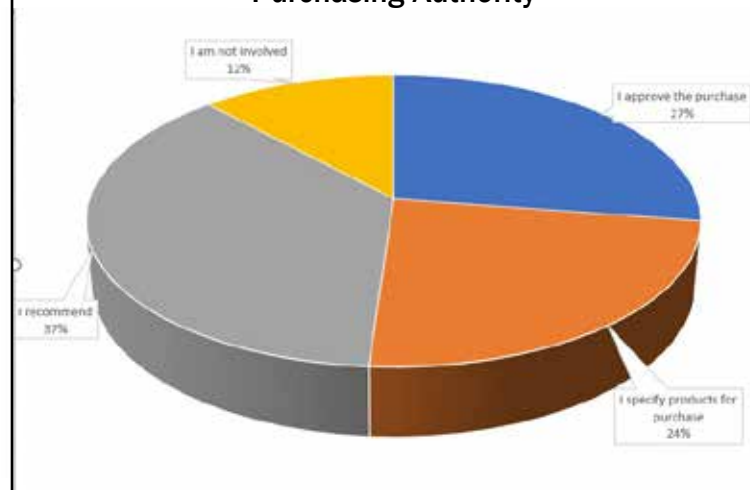


Statistics

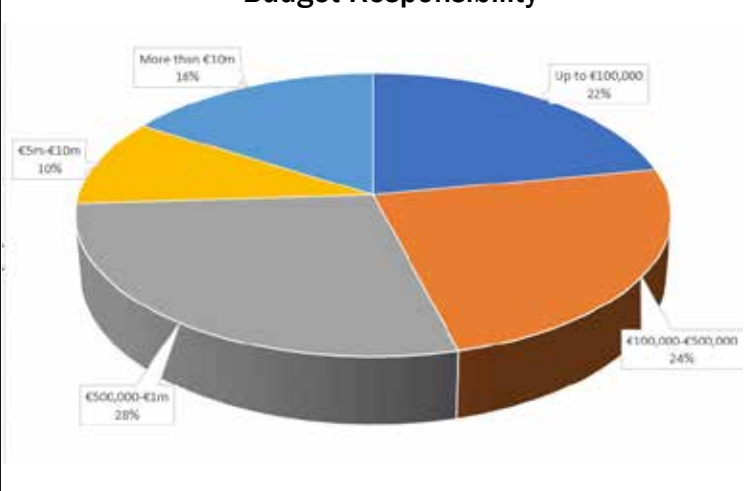
Organization Type



Purchasing Authority



Budget Responsibility



Why Attend

To find new solutions/new providers	42%
To learn more about the latest technologies and systems for protecting critical infrastructure facilities	51%
To network with peers and learn from others experiences	78%
To enhance my knowledge and understanding of threats, challenges and thought leadership in CI	67%
To listen to presentations from industry experts and peers	52%
To find new partners/customers, to create networks	17%

Critical Infrastructure Protection and Resilience Europe brings together leading stakeholders from industry, operators, agencies and governments to collaborate on securing Europe. 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.



critical infrastructure

PROTECTION AND RESILIENCE EUROPE

12th-14th NOV 2024

Madrid, Spain

www.cipre-expo.com

Critical Infrastructure Protection / Physical Security

Drone's, Insider threats, Vehicle Borne IED's, Suicide Bombers and Active Shooters are just some of the myriad of known threats facing CNI operators in 2024. Identifying ways of detecting, defeating and mitigating against those threats and building-in resilience are crucial organisation or CNI operator.

Combining CIIP/Cyber and Physical Security into one integrated strategy is not just desirable but crucial!

The Critical Infrastructure Protection & Resilience Europe exhibition will demonstrate and display some of the leading technologies, products and services available to the industry.

As an exhibitor you can meet leading decision makers from corporate and government establishments tasked with Critical Infrastructure Protection and Resilience.

Who is CIPRE for?

Critical Infrastructure Protection and Resilience Europe will attract:

- National government agencies responsible for national security and emergency/contingency planning
- Police and Security Agencies
- Emergency Services
- Local Government
- Facilities Managers – Nuclear, Power, Oil and Gas, Chemicals, Telecommunications, Banking and Financial, ISP's, water supply
- IT, Cyber Security and Information Managers
- Port Security Managers
- Airport Security Managers
- Transport Security Managers
- Event Security Managers
- Architects
- Civil Engineers
- EU
- NATO
- Military
- Border Officials

Who should Exhibit / Sponsor

Critical Infrastructure Protection and Resilience Europe provides great business development opportunities, as well as connections to a key target audience, for:

- OEM, Security equipment manufacturers and suppliers
- IT security providers and consultants
- Infrastructure protection consultants
- Facilities management companies
- Security Service providers
- Architects & Builders
- Civil Engineers

Critical Information Infrastructure Protection / Cyber Security

With the ever increasing threat from cyber attacks on critical infrastructure, the information and data stored and used by CNI systems and operators can be more crucial than the system itself. CIIP is becoming ever more important as part of the cyber security strategy of an organisation or CNI operator.

Benefits of Exhibiting/Sponsorship

- Build and enhance your company profile and image to key industry professionals
- Connect with customers and develop new business relationships
- Showcase your products and services to key decision makers and buyers
- Communicate your company's news and messages direct to your potential customers
- Learn about the latest challenges and threats facing the critical infrastructure sector
- Connect with more customers in less time in the best face-to-face environment

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

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

For conference or registration queries please contact:
Ben Lane
Event Manager
T: +44 (0) 7956 899806
F: +44 (0) 872 111 3210
E: benl@torchmarketing.co.uk



critical infrastructure

PROTECTION AND
RESILIENCE EUROPE

12th-14th NOV 2024

Madrid, Spain

www.cipre-expo.com

Why participate and be involved?

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

www.cipre-expo.com

Exhibiting Investment

The cost of participation at the Critical Infrastructure Protection & Resilience Europe is:

Table Top Exhibit - €2,950

2m x 1.5m raw space with 1 x table and 2 x chairs, 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

"Although the EC Directive has helped in 'assessing the need to improve the protection of European critical infrastructures' in the transport and energy sectors, there is no indication that it has actually improved security in these sectors."

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 below. Packages can be designed and tailored to meet your budget requirements and objectives. Sponsorship packages include a Table Top Exhibit.

Platinum Sponsor	Euro 12,500
Gold Sponsor	Euro 10,500
Silver Sponsor (2 available)	Euro 8,500
Bronze Sponsor (2 available)	Euro 6,500
Conference Videos and Proceedings	Euro 4,950
Delegate Folder Sponsor	Euro 4,950
Networking Reception Sponsor	Euro 3,950
Lanyard Sponsor	Euro 3,950
Badge Sponsor	Euro 3,950
Conference Proceedings Sponsorship	Euro 3,950
Delegate Restaurant Sponsor	Euro 3,950
Coffee Break Sponsor	Euro 3,950

For further details and to discuss,, contact your regional representative detailed below.

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 Europe please contact:

Ray Beauchamp -
Americas
E: rayb@torchmarketing.co.uk
T: +1-408-921-2932

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

Jina Lawrence
Rest of World
E: jinal@torchmarketing.co.uk
T: +44 (0) 7958 234750

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

Previous Delegates included:

- Director General, Fire Rescue Service of Czech Republic, Czech Republic
- Officer of the Crisis Management Department, Ministry of Industry & Trade, Czech Republic
- General Director, National Institute for Research and Development, Informatics ICI Bucharest, Romania
- Privacy and Security Officer, Alliander Telecom, Netherlands
- Strategy Consultant, Alliander Telecom, Nederland
- Head of Asset Protection, NS Corporate Security, Netherlands
- Senior Security Advisor, Chevron, United Kingdom
- Lead Expert Physical Security of Infrastructures, TUV Informationstechnik GmbH, Germany
- Head of Business Continuity Management, CEZ, Czech Republic
- General Secretary, EUTC, Belgium
- Security Manager, NAV Portugal, Portugal
- Deputy Senior Director, Energy and Nuclear Resources, Czech Republic
- CISO, Chief Deception Officer, State Treasury Shared Services Centre, Czech Republic
- Project Manager, Presidency of the Republic of Türkiye, Turkey
- Information Security Analyst, Saudi Aramco, Saudi Arabia
- Officer of the Crisis Management Department, Ministry of Industry & Trade, Czech Republic
- Aviation Security Consultant, Arup, UK
- Director of ITS, Ministry of Internal Affairs, Moldova
- Head of Industrial Risk Line, NIER Ingegneria S.p.A., Italy
- Entrepreneur in Residence, Telespazio Germany GmbH, Germany
- Senior Policy Advisor, Government of Canada, Canada
- Auditor, Energistyrelsen, Denmark
- CTO, Proxy Innovation Systems, Ghana
- Scientific Researcher, ICI Bucharest, Romania
- Associate Programme Officer, Organization for Security and Co-operation, Austria
- Ministerial Counsellor, Ministry of Transport, Czech Republic
- SENIOR RESEARCHER, ENGINEERING INGEGNERIA INFORMATICA S.P.A., Italy
- Business Information Security Officer, SLOVNAFT, a.s., Slovakia
- Tactical Specialist/Operator (Police), Royal Canadian Mounted Police, Canada
- Consultant, Ness, ISRAEL
- Secretary General, NEREUS aisbl, Belgium
- Group Chief Security Officer, GEOPOST GROUP, France
- Senior Cyber Security Solution Specialist, ESET, spol. s r.o., Slovak Republic
- Head of the Crisis Management Department, Ministry of Industry & Trade, Czech Republic
- OT Cyber Resilience & Cyber Security Architect, KPCS CZ, Czech Republic
- Sales Manager Drone Detection, Telespazio Germany GmbH, Germany
- Vice President of CS Operations and Scale Up, ESET, spol. s r.o., Slovak Republic
- CEER Market Lead, ESET, spol. s r.o., Slovak Republic
- Head of Major Risks Unit, NIER Ingegneria S.p.A, Italy
- Head of Air Defence Dept & Vice Dean for PR and Dev, Faculty of Military Technology, University of Defence, Czech Republic
- Country Director / CIDR Program, North Macedonia, DAI, North Macedonia
- Head of Application Systems and Technical Support Directorate, Information Technology Department of the Ministry of Internal Affairs, Moldova
- Head of Critical Infrastructure and Cultural, Ministry of the Interior, Civil Protection, Croatia
- Consultant, Ness, Israel
- CISO, TAQA Global, United Arab Emirates
- Security Expert, NAV Portugal, Portugal
- Senior Policy Advisor, Government of Canada, Canada
- Cybersecurity Solutions Engineer, Siemens Mobility GmbH, Germany
- Programme Manager - Transport Security, PA Consulting, UK
- TIEMS PRESIDENT, The International Emergency Management Society, Norway
- International Security Expert, TPASCO, Netherlands
- Head of Academy, F24 AG, Germany
- Research Fellow, Politecnico di Milano, Italy
- Senior Key Expert - Network Security, Siemens Mobility, Germany
- Director, TG Masaryk Water Research Institute, Czech Republic
- HEAD OF INTERNAL AUDIT, F.I.S. FABBRICA ITALIANA SINTETICI SPA, Italy
- Strategic Advisor, Idaho National Laboratory, United States
- Enterprise Security Architect, KPN, Netherlands
- Business Development Manager International, CRFS, UK
- Area Sales Representative, Betafence s.r.o., Czech Republic
- Researcher / Academical worker / Vice dean, Tomas Bata University, Cyprus
- Aviation Lead, National CT Security Office - NCTPHQ, United Kingdom
- "Cyber Security for Subsidiaries" Project Manager, AIRBUS SAS, France
- Auditor, Energistyrelsen, Denmark
- Section Manager - Crisis and Disaster Recovery Planning, Tools & Solutions, Saudi Arabia
- Office Manager, AIRPOL, Sweden
- Cybersecurity Architect, Airbus, France
- Senior Fusion Threat Intelligence Analyst, SecAlliance, United Kingdom
- Digital Marketing and Proposition Designer, ESET, spol. s r.o., Slovak Republic
- Regional Manager, Eastern Europe, Central Asia, and Türkiye, Iris ID Systems Inc, Turkey
- OT-Security Consultant, Omegapoint Stockholm, Sweden
- Research associate, GRS gGmbH, Germany
- Marketing Executive, CRFS, UK
- Security Expert, Consultant, Belgium
- CISO, INA-Industrija nafte, d.d., Croatia
- Kosovo Emergency Management Agency, Kosovo Emergency Management Agency, Kosovo
- Regional Sales Manager - East Central Europe, Genetec, France
- US Army, US Army, Germany
- Sales Executive, HSB identification B.V., Netherlands
- Lecturer, University of Central Lancashire, United Kingdom
- Managing Director, RAILPOL, Netherlands
- Secretary General, PESI, Spain
- Senior Key Account Manager, F24 AG, Italy
- Managing Director, GM Projekt d.o.o, Slovenia
- Senior Security Officer, eu-LISA, France
- President, AKICR, Czech Republic
- Senior Climate Scientist, Climate Service Center Germany / Helmholtz-Zentrum hereon, Germany
- Research Team Leader, DLR Institute, Germany
- Sales Representative, Betafence s.r.o., Czech Republic
- Head, AIRPOL, Sweden
- National Chengchi University, National Chengchi University, Taiwan
- Director, Ministry of Interior, Czech Republic
- Chairman of the Board T-SOFT, TIEMS Secretary, T-SOFT a.s., Czech Republic
- CHIEF COMMISSIONER, POLICE PRESIDUM OF THE CZECH REPUBLIC, DIRECTORAT, Czech Republic
- PROJECT OFFICER, EUROPEAN COMMISSION JOINT RESEARCH CENTRE, ITALY
- Senior Researcher, Politecnico di Milano, School of Management, Italy
- Head of CEE Sales and Product Development Strategy, Goldilock Secure Ltd, UK
- Secretary General, CoESS, Belgium
- Senior Research Scientist, Norwegian Computing Center, Norway
- Full Professor, VSB - Technical University of Ostrava, Czech Republic
- Aviation Lead, Unit Lead - Aviation & Maritime Security Unit - NaCTSO, United Kingdom
- Director, HSEMA, United States
- Key Account Manager - East Central Europe, Genetec, France
- Global Security Analyst, Chevron, United States
- Head of Security threats & Investigations, NS Corporate Security, Netherlands
- Research Assistant, University of Applied Science Magdeburg-Stendal, Germany
- Sales Engineer - East Central Europe, Genetec, France
- Director, Ministry of Interior, Czech Republic
- Tactical Liaison - Point Lepreau Nuclear Generating Station, Royal Canadian Mounted Police (RCMP), Canada



12th-14th NOV 2024

Madrid, Spain

www.cipre-expo.com

Madrid, Spain



Spain's critical infrastructure is the network of physical and cyber assets that are essential to the country's economy and security. It includes everything from power grids and water treatment plants to transportation systems and telecommunications networks. Critical infrastructure is essential for the delivery of essential services to the Spanish people and for the country's economic prosperity.

The security of Spain's critical infrastructure is a major challenge, given the country's strategic location and its exposure to a wide range of threats. These threats include:

- Natural disasters: Spain is prone to a variety of natural disasters, including earthquakes, floods, and wildfires. These disasters can cause significant damage to critical infrastructure, disrupting essential services and harming the economy.
- Terrorist attacks: Spain has been the target of several terrorist attacks in recent years, including the 2004 Madrid train bombings and the 2017 Barcelona attacks. These attacks have demonstrated the vulnerability of critical infrastructure to terrorist attacks.
- Cyberattacks: Spain is also increasingly vulnerable to cyberattacks. In recent years, there have been a number of high-profile cyberattacks on Spanish critical infrastructure, including the 2017 WannaCry ransomware attack and the 2020 SolarWinds hack. These attacks have shown how cyberattacks can disrupt critical infrastructure and cause significant economic damage.

The Spanish government has taken a number of steps to improve the security of its critical infrastructure. These steps include:

- Establishing a national critical infrastructure protection strategy: The Spanish government has established a national critical infrastructure protection strategy that outlines the government's approach to protecting critical infrastructure. The strategy focuses on four key areas: risk assessment, prevention, detection and response, and recovery.
- Creating a national cybersecurity center: The Spanish government has created a national cybersecurity center (CNNC) to coordinate cybersecurity efforts across the government and the private sector. The CNNC is responsible for monitoring cyber threats, providing incident response support, and raising awareness of cybersecurity issues.



For further details visit www.cip-association.org
or email info@cip-association.org.

International Association of CIP Professionals (IACIPP)

The IACIPP is a global fraternal association of CIP professionals, dedicated to sharing ideas, information, experiences, technology and best practice, with the express purpose of making the world a safer place.

The association is open to critical infrastructure operators and government agencies, including site managers, security officers, government agency officials and policy makers. The purpose is to share ideas, information, experiences, technology and best practise.

The Association, although very young in its journey, is clear in what it is seeking to achieve. The creation of a network of like minded people who have the knowledge, experience, skill and determination to get involved in the development and sharing of good practice and innovation in order to continue to contribute to the reduction of vulnerabilities and seek to increase the resilience of Critical Infrastructure and Information.

The IACIPP initial overall objectives are:

Benefits of Membership include:

- Developing access to training programmes, courses and qualifications
- Enabling and ensuring the Continual Professional Development of industry professionals
- Participate in setting direction of IACIPP
- Access to Members Intranet Site
- Access to communal LinkedIn group
- Vote for IACIPP and officers (only members are allowed to become part of the Executive Committee and serve as Officers of the Association)
- Discounted delegates fees for CIPRE, CIPRA and CIPRNA
- Voting for annual industry and operator awards
- Access to internet roundtable discussions
- Developing working groups – with specific purpose and agenda's
 - Transport
 - Energy
 - Telecomms
 - Cyber/CIIP/IT Infrastructure
 - Water



- To develop a wider understanding of the challenges facing both industry and governments
- To facilitate the exchange of appropriate infrastructure & information related information and to maximise networking opportunities
- To promote good practice and innovation
- To facilitate access to experts within the fields of both Infrastructure and Information protection and resilience
- To create a centre of excellence, promoting close co-operation with key international partners
- To extend our reach globally to develop wider membership that reflects the needs of all member countries and organisations

The Association also aims to:

- Provide proactive thought leadership in the domain of critical infrastructure security and resilience.
- Help set the agenda for discussions in infrastructure security and resilience
- Promote and encourage the sharing of information, knowledge and experience that will enhance security.
- To filter, collect, collate and co-ordinate information and data sharing.
- Identify and promote new technologies that can enhance security and resilience.
- Share information with members about the changing threat landscape
- Share information, ideas and knowledge to promote best practice
- Educate operators and provide industry standards
- Act as a Liaison between operators, government, intergovernmental bodies
- Make available surveys and research
- Provide the mechanism for liaison between operators and industry

How to Join:

IACIPP has been developed for representatives from government, agencies and operators tasked with security, protection and resilience of CNI.

If you are interested in membership please contact us at info@cip-association.org or visit www.cip-association.org

Flagship Media Partner:

critical infrastructure PROTECTION AND RESILIENCE NEWS

Critical Infrastructure Protection & Resilience News (CIPR News) is a quarterly digital newsletter distributed to over 85,000 subscribers globally.

CIPR News focusses on core security issues and news covering critical infrastructure and its sub-sectors.

CIPR News is the official magazine of the International Association of Critical Infrastructure Protection Professionals (IACIPP).

SHARE YOUR NEWS

Through our dedicated media channel of CIPR ENews, we invite our industry partners to share news about products, product developments and contracts with us and our stakeholders 24/7 365 days a year.

Editorial Contact

Neil Walker
Director - IACIPP
E: neilw@cip-association.org

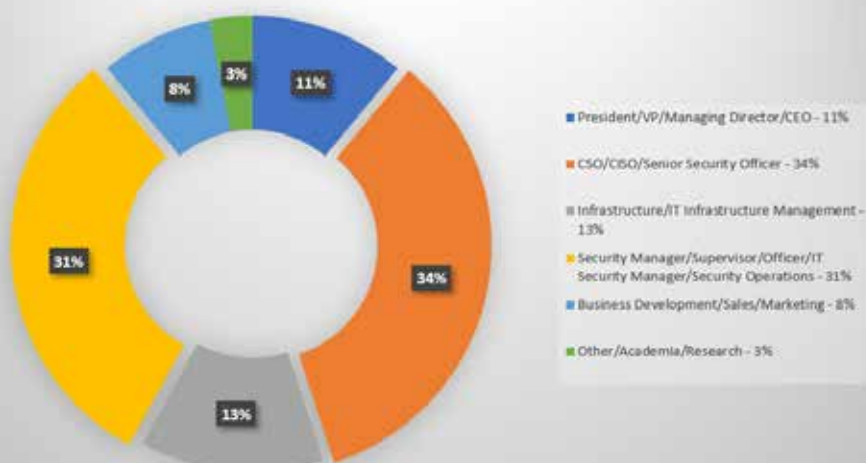


critical infrastructure PROTECTION AND RESILIENCE NEWS



Circulated globally to over 85,000 infrastructure operator/owners, agencies, law enforcement, federal and state government and industry experts, as well as members of IACIPP.

Job Function



85,000+ circulation

largest circulation magazine for CIPR industry.

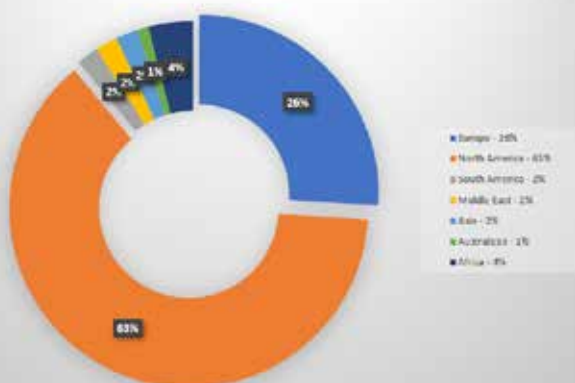
Targeted marketing

offering you great opportunities highly targeted campaigns to the Critical Infrastructure Protection & Resilience industry

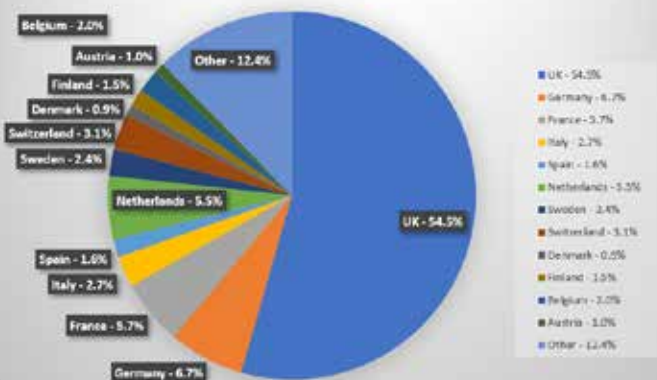
To find new solution providers

discover news, views, stories and latest products and solutions are the biggest reasons people read CIPR News

GEOGRAPHIC



Europe Breakdown



EDITORIAL CALENDAR

What your clients will be reading

Spring 2024

- Emergency Preparedness
- Airport & Aviation Security
- Emergency Preparedness
- Power, Energy & Grid Resiliency
- News and Views from the Agencies
- Critical Infrastructure Protection and Resilience North America Preview
- Industry and technology news

Bonus distribution:

Critical Infrastructure Protection and Resilience North America;
World Border Security Congress

Ad Deadline: 5th February 2024

Summer 2024

- Cybersecurity
- Critical Information Infrastructure Protection
- Critical Industries Security
- Strategic Resilience Planning
- News and Views from the Agencies
- Critical Infrastructure Protection and Resilience North America Review
- Industry and technology news

Bonus distribution:

TBA

Ad Deadline: 13th May 2024

Autumn 2024

- Space as Critical Infrastructure
- Transport Security
- Incident Mitigation & Emergency Management
- CER & NIS2 Directive Updates
- News and Views from the Agencies
- Critical Infrastructure Protection and Resilience Europe Preview
- Industry and technology news

Bonus distribution:

TBA

Ad Deadline: 9th September 2024

Winter 2024

- Critical Infrastructure Interdependencies and Cascading Effects
- Communications Sector Security and Resilience
- The Insider Threat
- Public Private Partnerships
- News and Views from the Agencies
- Critical Infrastructure Protection and Resilience Europe Review
- Industry and technology news

Bonus distribution:

Critical Infrastructure Protection and Resilience Europe;
International Security Expo

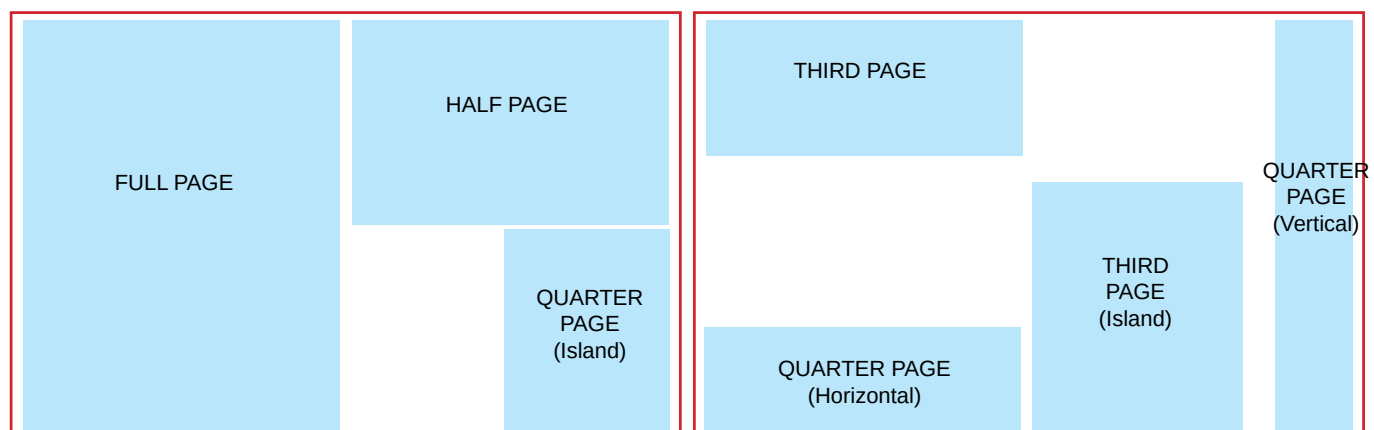
Ad Deadline: 2nd December 2024



PRINT MEDIA ADVERTISING RATES AND SPECIFICATONS

DISPLAY						
	1x		3x		6x	
Full page	£1,670	\$2,150	£1,545	\$1,975	£1,420	\$1,825
Half page	£1,250	\$1,600	£1,150	\$1,450	£1,045	\$1,325
Third page	£1,050	\$1,350	£960	\$1,225	£875	\$1,100
Quarter page	£835	\$1,050	£795	\$1,000	£750	\$950

DISPLAY	STANDARD SIZES (W x H)	
Magazine	Trim size	210mm x 297mm (A4)
Full page	Bleed	216mm x 303mm
Full page	Live area	190mm x 277mm
Half page	Island	115mm x 190mm
Half page	Horizontal	190mm x 138mm
Half page	Vertical	92mm x 277mm
Third page	Square	115mm x 115mm
Third page	Horizontal	190mm x 99mm
Third page	Vertical	60mm x 277mm
Quarter page	Island	92mm x 138mm
Quarter page	Vertical	45mm x 277mm
Quarter page	Horizontal	190mm x 68mm
Double page spread (3mm bleed head, foot and face only)	Spread	420mm x 297mm (426mm x 303mm)
Half page spread (3mm bleed foot and face only)	Spread	420mm x 145mm (426mm x 148mm)



critical infrastructure PROTECTION AND RESILIENCE NEWS



International Association of
CIP Professionals

For the latest news from industry and government on security,
protection and resilience on CNI

FOLLOW US



SEPTEMBER 2020



HEADLINE NEWS

Climate change-fueled weather disasters: Costs to state and local economies

The US Government Accountability Office (GAO) estimates that between 2005 and 2019, the federal government, including FEMA and other agencies, has spent at least \$450 billion on weather disaster assistance, an average of \$30 billion per year (GAO 2019). It is easy to imagine that, in the face of the COVID-19 pandemic, a similar level of aid may not be available for weather disaster assistance.



[Read more >>](#)

Policy brief: technologies for averting, minimizing and addressing loss and damage in coastal zones

Coastal zones are home to about 40 per cent of the world's population, living within 100 km of the coastline. The most recent technology needs assessment indicates that one-third of developing countries placed infrastructure, including in coastal zones, as a prioritized sector, and most of the prioritized technologies in this regard were related to coastal protection, including both hard and soft measures.



[Read more >>](#)

JOIN US TODAY

The International Association of CIP Professionals aims to share ideas, information, experiences, technology and best practice on many of the serious Infrastructure - Protection - Management and Security issues challenges - facing both Industry and Governments. Learn more on the [aims](#) and [objectives](#) of the Association and [Join Today](#) and play an active part in developing and shaping the industry.



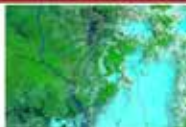
[Read more >>](#)



MORE NEWS

Record floods threaten nuclear power site in Bangladesh

Bangladesh has experienced intense flooding covering at least a quarter of the country as it goes through monsoon season. NASA has released a map showing the extent of this year's flooding from June to the end of July along the Jamuna River, where high danger levels have been reached or surpassed. Reported at the end of July, more than 4.7 million people have been affected and more than half of Bangladesh's districts are flooded.



IACIPP ENews is the monthly ENewsletter of the
International Association of CIP Professionals,
circulated to 80k industry professionals globally.

Premium position - Horizontal

728 x 90px

1 month	3 months
£625 \$750	£545 \$650
6 months	12 months
£500 \$600	£460 \$550

Mid position - Horizontal

728 x 90px

1 month	3 months
£500 \$600	£460 \$550
6 months	12 months
£420 \$500	£375 \$450



DIGITAL MEDIA ADVERTISING OPPORTUNITIES

EVENT WEBSITE BANNER

Premium position - Horizontal

728 x 90px

1 month	3 months
£310 \$375	£275 \$335
6 months	12 months
£250 \$300	£230 \$280

Square banner

125 x 125px

1 month	3 months
£150 \$170	£130 \$150
6 months	12 months
£115 \$135	£100 \$120

EVENT ENEWSLETTER

CIPRNA and CIPRE events monthly ENewsletter is circulated to industry professionals across their appropriate geographic regions and interested CIPR organisations and developments.

Premium position - Horizontal

728 x 90px

1 month	3 months
£310 \$375	£275 \$335
6 months	12 months
£250 \$300	£230 \$280

Mid position - Horizontal

728 x 90px

1 month	3 months
£250 \$300	£230 \$280
6 months	12 months
£210 \$260	£190 \$240

DIGITAL MEDIA ADVERTISING OPPORTUNITIES

WEBINARS

Hosted by CIPR ENews. Moderated interview style webinar with 2-4 speakers supplied by the sponsor. Topic driven by sponsor. Program approx 45 minutes in length. Audio with power point. Power point provided by Sponsor. The sponsor of the webinar and their speakers will be featured in all of the promotional efforts:

What CIPR/NA/E and CIPR ENews will do:

- Email Blast – several DEDICATED EMAIL blasts to 85,000+ contacts. Typically, two prior and one post live event.
- Website – Home page banner on our web sites with click through to the webinar
- Push Notices – to our LinkedIn Groups
- Banners in our monthly e-newsletter. Typically, two prior and one post live event.
- Advert Specifically for the webinar in CIPR ENews
- Registration engine to capture details of those who register for the webinar.
- Details of those who registered for the webinar provided in a spreadsheet to Sponsor.

What will be needed from the Sponsor:

- a topic
- a power point presentation
- 2-3 speakers
- at least one phone call ahead of time with all speakers.

Once delivered, either live or using a pre-recording, the webinar remains available online on-demand and future subscribers are passed on to you.

Cost £2,950.00 (\$3,750) for the live webinar which will also remain on the site for a full 12 months



Further Information

If you are interested in exhibiting and sponsorship opportunities at the Critical Infrastructure Protection & Resilience News please contact:

Ray Beauchamp -
Americas
E: rayb@torchmarketing.co.uk
T: +1-408-921-2932

Jina Lawrence
Rest of World
E: jinal@torchmarketing.co.uk
T: +44 (0) 7958 234750

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

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



critical infrastructure

PROTECTION AND RESILIENCE AMERICAS

March 12th-14th, 2024
LAKE CHARLES, LOUISIANA
www.ciprna-expo.com

critical infrastructure

PROTECTION AND RESILIENCE EUROPE

12th-14th November 2024
Madrid, Spain
www.cipre-expo.com



Further Information

If you are interested in exhibiting and sponsorship opportunities at the Critical Infrastructure Protection & Resilience North America or Europe please contact or complete the form and return to:

Ray Beauchamp -
Americas
E: rayb@torchmarketing.co.uk
T: +1-408-921-2932

Jina Lawrence
Rest of World
E: jinal@torchmarketing.co.uk
T: +44 (0) 7958 234750

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

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

Name: _____

Job Title: _____

Organisation: _____

Address: _____

Town/City: _____

County/State: _____

Postcode/ZIP: _____ Country: _____

Tel: _____

Fax: _____

Email: _____

Please tick if you do not wish to be contacted by:
Tel: ☐ Fax: ☐ Email: ☐ Mail: ☐

Data Protection: Personal Data is gathered in accordance with the Data Protection Act 1998.

Critical Infrastructure Protection & Resilience events are owned and organised by Torch Marketing.
Queries relating directly to the event should be directed to Torch Marketing, info@torchmarketing.co.uk.