

# critical infrastructure



## PROTECTION AND RESILIENCE NEWS

Official Magazine of



WINTER 2023/24  
[www.cip-association.org](http://www.cip-association.org)

### FEATURE:

**Protection of the EU's Critical Infrastructure: Evaluation of new legal instruments**

### FEATURE:

**CIP: coming of age, facing new challenges**

### FEATURE:

**Enhancing Security Through Integration: The Crucial Role of Integrating Physical Security Systems**



# EYES ON CYBER IN THE MARITIME FIELD





Co-Hosted and Supported by:



# critical infrastructure PROTECTION AND RESILIENCE AMERICAS

March 12<sup>th</sup>-14<sup>th</sup>, 2024  
LAKE CHARLES, LOUISIANA

*A Homeland Security Event*

## Collaborating and Cooperating for Greater Security

*For Securing Critical Infrastructure and Safer Cities*

## Register Today

**SPECIAL DEAL FOR INFRAGARD LA MEMBERS, GOVERNMENT AND OWNER/OPERATORS**

For further details and to register visit [www.ciprna-expo.com/registration](http://www.ciprna-expo.com/registration)

The latest Critical Infrastructure Protection and Resilience North America brings together leading stakeholders from operator/owners, agencies, governments and industry to debate and collaborate on securing America's critical infrastructure.

As we come out of one of the most challenging times in recent history, it has stressed how important collaboration in protection of critical infrastructure is for a country's national security.

Agenda includes Industry Sector Mini Symposiums to focus on your specific CI sector, with the enhanced opportunity to discover and share experiences across these sectors:

- Power & Energy (Grid Resilience) Sector Symposium
- Pipelines Sector Symposium
- Transport Sector Symposium
- Critical Industries Sector Symposium
- Communications Sector Symposium
- CIIP / Cybersecurity Sector Symposium

Join us in Lake Charles, LA, USA for the premier event for operator/owners and government establishments tasked with the region's Critical Infrastructure Protection and Resilience.

*Leading the debate for securing America's critical infrastructure*



**REGISTER ONLINE AT [www.ciprna-expo.com/registration](http://www.ciprna-expo.com/registration)**

### Opening Keynote:

- Dr David Mussington, Assistant Director, CISA

### Confirmed speakers include:

- Budge Currier, Assistant Director Public Safety Communications, California Office of Emergency Services (Cal OES)
- Brian Harrell, Vice President and Chief Security Officer (CSO), Avangrid, USA
- Charles Burton, Technology Director, Calcasieu Parish, USA
- Lester Millet, Policy & Planning Director and Safety Risk Agency Manager, Port of South Louisiana & President, Infragard Louisiana
- Jeff Gaynor, President, American Resilience, USA
- Ron Martin, ICAM-Critical Infrastructure, Capitol Technology University, USA
- Tim Klett, Strategic Technology Integration Strategist, Idaho National Laboratory, USA
- Emilio Salabarría, Senior Program Manager for Cybersecurity, The Florida Center for Cybersecurity: Cyber Florida
- Chris Janson, Sr. Market advisor, Nokia, USA
- Rola Hairi, Defense Industrial Base Sector Liaison, Cybersecurity and Infrastructure Security Agency (CISA)
- Richard Tenney, Senior Advisor, Cybersecurity, Cybersecurity and Infrastructure Security Agency (CISA)
- Michael Finch, Technology Services Director, Lane County Department of Technology Services
- Jim Henderson, CEO, Insider Threat Defense Group, Inc., Founder / Chairman, National Insider Threat Special Interest Group

For speaker line-up visit  
[www.ciprna-expo.com](http://www.ciprna-expo.com)

## ARE WE PREPARED FOR THE INEVITABLE?

March will see the 2024 Critical Infrastructure Protection & Resilience North America take place in Lake Charles, Louisiana, and the next gathering opportunity for those involved in the protection, security and resilience of critical infrastructures and assets. An opportunity to catch up and share experiences, knowledge and skills, and an more importantly to collaborate and cooperate in the challenging times in which we currently live.

Threat vectors seem to be increasing, as the developing situations in the Middle East and Russia/Ukraine increase tensions and rhetoric from our politicians. It is an important time for level heads and our intelligence services to be providing the right level of information to our security officers for being able to better plan and prepare.

In Europe the implementation of the Critical Entities Directive will see the need for CIP operators and agencies meet minimum standards of protection and resilience come in to force, with penalties for those failing to meet these standards. Together with the NIS2 Directive, these are meant to provide high standards to ensure resilience in the system, but with the continuous and emerging threats and escalation of cyber attacks, will these minimum standards be sufficient, and are we prepared for the worst?

In this issue we find some excellent contributions from a range of experts in the CI field, which we hope you will find interesting and enlightening.

Expect the best, plan for the worst, and prepare to be surprised. Although we can gain some insight into the developing world, through intelligence and analysis, we cannot be certain of what is around the corner. One thing for sure is something will happen, and we need to be prepared.

Enjoy this issue of Critical Infrastructure Protection & Resilience News and we hope to welcome you to Lake Charles on 12th-14th March at CIPRNA 2024.

Thank you.

[www.cip-association.org](http://www.cip-association.org)

**Editorial:**

Neil Walker

E: [neilw@torchmarketing.co.uk](mailto:neilw@torchmarketing.co.uk)

**Design, Marketing & Production:**

Neil Walker

E: [neilw@torchmarketing.co.uk](mailto:neilw@torchmarketing.co.uk)

**Critical Infrastructure Protection & Resilience News** is the newsletter of the International Association of CIP Professionals and distributed to over 80,000 organisations globally.



## Eyes on Cyber in the Maritime field



By Adrian Victor Vevera – General Director of the National Institute for Research and Development in Informatics ICI Bucharest, PhD. Eng., Nuclear Physicist by training, Scientific Researcher 2 title in the Romanian research establishment

The sinews of the world are straining and we have seen it takes little for them to break

It gives one a feeling a déjà vu to witness another reminder of the essential vulnerability of the global logistics chain making possible the globalized world, its division of labor and its abundance of products for every season and market. Rightly, people are concerned about the Yemeni



Adrian Victor Vevera – General Director of the National Institute for Research and Development in Informatics ICI Bucharest

rocket attacks on commercial shipping crossing the Bab-el Mandeb Straits and the Red Sea on their way to and from mainly Europe, carrying fuel, foodstuffs, and manufactured products. People are also concerned that the roundabout alternative around the Cape of Good Hope adds time and costs to shipping, thereby reducing efficiency and the overall capacity of the system. Whatever initiative the militaries of interested powers



put into motion, it must not only deter attacks but also reassure civilian shippers, their clients upstream and downstream, their insurers and other actors that this security is sound.

However, I find it hard to take seriously the shock emanating from certain quarters that funneling most of global maritime trade by tonnage through a few key chokepoints would result in vulnerabilities that certain actors would take advantage of. In other words, it is a systemic vulnerability exploited by a threat actor to coerce the affected parties through the impact on the system-of-systems that literally makes modern supply and production chains possible. And we have been consistently forewarned, if not forearmed, that maritime trade and, by extension, maritime infrastructures, assets, and organization, is an immensely complex integrated critical infrastructure which is tightly wound and relatively easily perturbed. Off the top of my head, I will list the Ever Given blockage of the Suez Canal in March 2021, the horrendously complex impact of the pandemic and the anti-pandemic measures on transport capacity worldwide, and the impact of Russia's blocking of the Ukrainian maritime grain transport routes as examples.

And I want to take this opportunity to underscore a different kind of threat, no less insidious, costly, or deadly, to the critical infrastructure that makes possible the global production and supply chains on which we rely – the cybersecurity of the maritime domain. This is, without hyperbole, a threat that knows no borders or chokepoints,



that is omnipresent, that affects all aspects of the value chain, and that entails a complex ecosystem of aggressors, from states and state proxies, to rivals, criminal groups, terrorist organization or ideological actors. And the cost to benefit ratio of attacks through cyber vectors is so good, and the barriers to entry for new aggressors are so low (relatively), that we can anticipate that the situation will get worse. This is not helped by the rapid pace of digitalization, which is driven by new systems, practices, and standards in relation to new ship classes and other assets that are meant to increase capacity, decrease labor as a component, increase energy efficiency, environmental friendliness and more. The tradeoffs are all in the direction of heightening cyber risk.

#### The issues at play

The term OT (operational technology) has developed to encompass a wider array of technologies and applications than industrial control systems, while still representing, according to the renowned consultancy Gartner, "hardware and software that detects or causes a change

through the direct monitoring and/or control of physical devices, processes, and events in asset-centric enterprises, particularly in production and operations." The proliferation of cyber-physical systems which interact with the physical world through the cyber environment, has created a whole new playhouse for the hacker or the complexity-driven disruption. In contrast to traditional "industrial" entities running ICS, asset-centric entities in the maritime sector feature significant distinctions and challenges, such as wide distribution of assets, cross-border nature of operation and governance, more frequent and complex interactions with other entities and their particular systems, as well as a greater intrusion of geopolitics and geoeconomics into the mix. So far, so well, but new digital paradigms, such as the Internet-of-Things moving from our wearable devices into the industrial area, have resulted in a rapidly changing cybersecurity landscape. This is especially true for the maritime domain, where the IoT paradigm facilitates cheap, accessible, and sustainable control systems in

## Vital Integrators As Your Business and Technology Partner

### Vital Managed - Fully Managed Services

Custom solution perfect for companies and organizations that want to outsource all aspects of technology. This solution is for those organizations that do not have a technical team or want a hands off approach to managing IT needs and infrastructure. Helpdesk, licensing, and network hardware can all be bundled so you pay one convenient price without variable costs each month. Leave the headache of IT management to us!

#### What's Included:

- Everything from Vital Secured Plan

#### Plus:

- Unmetered Support Hours (M-F)
- Office 365 Premium Licensing or Equivalent
- Enterprise Cloud File Server (not Dropbox/Sharepoint)
- Inventory and Warranty Tracking
- Mobile Device Management As Needed
- Employee Onboarding and Offboarding Assistance
- Ticket Portal and End User Submission from Device

#### Optional Add Ons:

- Network Hardware and Licensing
- Phone Systems
- Security Camera Systems
- Specific Office 365 Application Licensing (Visio, Project, Power BI etc)

#### What's Not Included:

- Projects such as whole office moves
- Unplanned Server Upgrades or Migrations
- Mileage or travel expenses
- Proprietary or customized software licenses (Adobe, Autodesk, Quickbooks etc)
- Additional Users or devices would be additional fee per month.
- After Hours / Holiday requests

**Cyber Security and IT Management  
done FOR you.**



### Vital Secured - Co-Managed Services

Custom solution tailored to companies and organizations that have an internal IT team but desire to compliment internal team with cyber security protections and 24/7 staffed security operations center. Also needing assistance with high level technology issues along with business roadmap and project support. Pay one convenient price for security peace of mind and only pay for hours needed at a discounted rate.

#### What's Included:

- 24/7 Security Operations Center
- Always on VPN Client, no more logging in or losing passwords
- Email Filtering Including Attachment Scanning and Link Verification
- DNS Filtering Services
- Advanced Anti-Virus (EDR)
- Monitored Anti-Virus with staffed SOC team
- Next Generation Firewall Logging Reviewed for Security Threats
- SIEM Ingestion and Analysis
- Zero Trust Network Option
- Office 365 Security Alerting and Remediation
- Complete EDR Solution
- Operating System Security Updates
- Windows and Mac Services Available
- 2FA Management and Enforcement
- Password Management Solution
- Ongoing Security Audits
- Cyber Security Training for Staff
- Email Backups Including Shared Mailboxes and Teams
- Dark Web Monitoring and Alerting
- Detailed IT Documentation Shared with Internal Staff
- vCIO Services

#### Optional Add Ons:

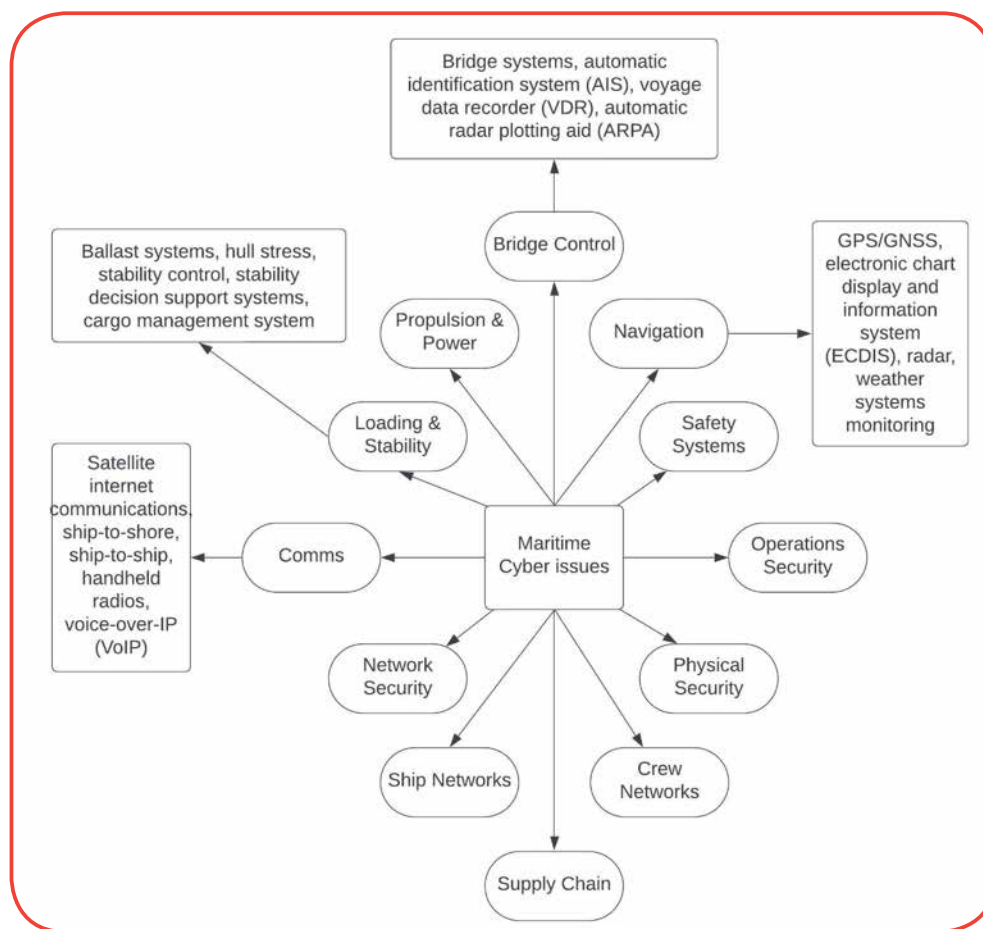
- Office 365 or Equivalent
- Enterprise Cloud File Server (not Dropbox/Sharepoint)
- Network Hardware and Licensing
- Mobile Device Management
- Phone Systems
- Security Camera Systems
- Specific Office 365 Application Licensing (Visio, Project, Power BI etc)

#### What's Not Included:

- All hours for service requests billed at discounted hourly rates
- Mileage or travel expenses
- Proprietary or customized software licenses (Adobe, Autodesk, Quickbooks etc)
- Additional Users or devices would be additional fee per month.

**Cyber Security and IT Management  
done WITH you.**

Every package is custom designed to meet your specific needs, call us at **337-313-4200** to build your solution!



*Figure 1. The maritime cyber domain – key components and issues*

highly distributed geographic environments, with real-time analytics, sophisticated embedded systems, cloud storage and computing, and commercial-off-the-shelf sensors.

Figure 1 is an attempt to provide a snapshot of the complicated cyber domain metasystem for the maritime, involving the assets but also the organizations and the facilities required. We can observe that there are important specificities in play that warrant the particular attention given to the cyber maritime domain as its own field. Firstly, there are numerous domains in which cyber threats are felt, particularly as air-gapped digital systems gave way to networked systems facilitating a downsizing of the crew and more efficient use of the asset or the shore facilities (such as container loading and unloading). These vary depending on the entity, region, or asset in question, but the razor-thin margins of competitive maritime transport drive those unwilling to adapt out of the business. Digitalization becomes not just a growth strategy, but an economic survival strategy. Maritime actors rely on dedicated systems, which the figure tries to underline, for instance in communications, identification, displays, data recording, radar plotting and more. Specific systems that are not

usually of concern in terrestrial settings are also important, such as engine control, ballast, stabilization. Decision support systems will become even more important as unmanned shipping fleets come online chasing new efficiencies. Many of these issues are relevant in other maritime-specific areas such as offshore infrastructures like oil rigs, offshore wind farms and others. The newer generation of offshore infrastructure, including tethered floating wind turbines, require active stabilization and careful environmental monitoring to maintain safety and security. With Europe looking to power through to energy independence partly through renewables, offshore infrastructure will become a more and more important component of this strategy.

### High profile cases

Basically, the surface contact area between the maritime domain and the cyber environment is growing, driven not just by digitalization, but also by greater networking in service of distributed command, control, and coordination systems. We have seen this in play several times in recent history and the threat actors are not just "growing their business", but choosing to enhance their aggression right when the circumstances guarantee maximum disruption. The start of the pandemic saw restriction efforts which put pressure on logistical systems which atrophied in the lockdown and were overstrained in the post-lockdown economic bounce. Between February and June 2020, Israeli consultancy Naval Dome reported a 400% increase in cyber-attacks against shipping. There was an across the board increase in attacks, but the maritime domain certainly saw some of the worst dynamic, perhaps second to the critical health infrastructures.

In June 2017, Maersk was affected by NotPetya, a ransomware analogue malware that did not spread through social engineering or spam, which burned through Maersk in seven minutes. Maersk lost all its data, 49,000 laptops and 4,000 servers, with direct damages totaling 300 million dollars. One office alone was spared through an unrelated power outage.



In 2018, the Chinese company COSCO was affected by the SamSam ransomware which eschews the commodity and malware-as-a-service approach of others in favor of in-house development to respond to security updates and other issues. COSCO reported effects in the United States, Canada, Panama, Argentina, Brazil, Peru, Chile, and Uruguay. It did not disclose the damages, but it boasted a return to normalcy in five days, through its use of segmented networks, backups for data and contingency plans.

Allianz's 2023 Safety and Shipping Review pointed out that many attacks target onshore components of maritime infrastructures and cited attacks in 2022 against the Port of London Authority and the Port of Los Angeles, and attacks in 2023 against the Port of Halifax and the ports of Montreal and Quebec. This just means that there is room to grow for hackers targeting the ships themselves and a January 2023 cyber-attack against DNV, a software vendor offering a ShipManager software, affected 1,000 ships and required a server shutdown.

#### **The response is not easy**

Getting ready is not easy, especially in the absence of some technical silver bullet. The C-suite and other stakeholders must have a vision regarding the creation of a cybersecurity strategy, its implementation, the adequate sourcing of technology, of security products and services, of intelligence on the threat environment affecting the entity and its supply chain, but also a discipline in developing, updating, and practicing contingency plans.

Companies must perform risk assessments, they must educate staff, promote cybersecurity hygiene, and take a good hard look at the various surprises that they may find, such as bad practices from work-from-home staff, unpatched software and operating systems, access management issues, third party vendor risks etc. This is not helped by economic pressure which saw a possible decrease in budgets dedicated to cybersecurity for industrial control systems and operational technology in 2023, according to a SANS Institute survey in 2023. It is not just about the money, there has to be a strategic cyber culture in the entity that facilitates adaptation to the new reality, otherwise we will keep facing the issue pointed out by the Safety at Sea and BIMCO Maritime Cyber Security survey, which said that 77% of its respondents thought that cyber-attacks were a medium to high risk, but only 42% actually had OT-security in place, 62% had some contingency plans and only 24% actually tested them every three months (15% tested them every six months).

Awareness is growing, not just from industry actors, but also from other stakeholders. New developments in critical infrastructure governance in Europe, such as the Critical Entities Resilience Directive and the NIS 2 Directive, help, although dedicated maritime infrastructure or maritime cybersecurity frameworks elude European decision makers. I can report, through the experience of my institute, a growing awareness of the importance of protecting the maritime domain from hybrid threats. May 2023 saw a European Defence Agency tabletop exercise on critical energy infrastructure

security against hybrid threats with an important maritime component take place in Sofia, with an expert from ICI Bucharest in the organizing committee and coordinating one of the exercise groups. The exercise was especially interested in exploring the reaction of stakeholders to threats expressed in the maritime domain through a cyber vector and successfully raised awareness of a host of issues related to maritime and energy. ICI Bucharest will also have a representative in the "Cyber Security Incident Response Exercise: Constanta Port" scheduled for February 21 and 22, 2024 in Constanta, Romania. This tabletop exercise will be organized by the Maritime Cybersecurity Centre of Excellence at the Constanta Maritime University, in partnership with the Romanian National Cyber Security Directorate, aiming to promote collaboration, improve communication and enhance problem-solving capabilities in the realm of cybersecurity. The Black Sea region is, for many reasons, both structural/long-term and related to the conflict in Ukraine, a petri dish for all manner of hybrid threats, including cyber maritime issues. Decision makers and other stakeholders try to get to grips with the rapidly changing security environment and to get ahead of threat actors in order to promote resilience in the maritime domain. Cyber resilience will have to be a part of it because, while the Houthi forces will eventually be silenced in their assaults on neighboring trade routes, there is nothing stopping the long march of cybercrime and cyber warfare through our critical infrastructures and our assumptions about our level of security.



## DOE announces \$30 million funding for cybersecurity tools to protect clean energy infrastructure

The Office of Cybersecurity, Energy Security, and Emergency Response (CESER) within the U.S. Department of Energy (DOE) has released a US\$30 million funding opportunity (FOA) for research, development, and demonstration (RD&D) of cybersecurity tools and technologies to protect clean energy infrastructure. The Cyber RD&D FOA for Clean Energy Infrastructure supports CESER's ongoing work to develop next-generation technologies to protect the nation's clean energy infrastructure from increasing cyber threats.

Earlier, the DOE announced that it has granted up to \$70 million in funding to support research into technologies designed to increase resilience and reduce risks to energy delivery infrastructure from a variety of hazards, including cyber and physical threats, natural disasters, and climate-change fueled extreme weather events.

"America's energy delivery infrastructure is critical to our overall national and economic security," David Crane, DOE Under Secretary for Infrastructure, said in a media statement. "This funding will

drive the development of next-generation cyber technologies that keep our nation at the forefront of innovation while protecting our energy infrastructure from increasing cyber threats. This work could not be more important or timely as our nation transitions to the clean energy economy."

The CESER will fund the research and development of new tools and technologies to detect and mitigate cyber threats to clean energy delivery infrastructure, including cloud infrastructure that underpins modernization.



**Security solutions**  
to protect your perimeter,  
facilities and people.

Join JCI Security Products at booth #19  
to learn more.

American Dynamics

Software House

Illustra



## Bhutan is protecting its vital infrastructure systems by strengthening resilience to disasters

Fourteen agencies working in the critical infrastructure sectors in Bhutan met with a shared commitment to strengthen infrastructure resilience through the project entitled 'Resilience of infrastructure through enhanced governance'.

Bhutan faces escalating challenges from natural and human-made hazards, including earthquakes, floods, landslides, glacial lake outburst floods and forest fires. The country's vulnerability to these threats is compounded by an increasingly complex disaster risk landscape driven by climate change. This places a growing number of people, assets, and livelihoods at compounded risk and generates potential cascading impacts on diverse segments of Bhutanese society.

To address these risks, a team of experts from project partners – the Coalition of Disaster Resilient



Infrastructure (CDRI) and the United Nations Office for Disaster Risk Reduction (UNDRR) - joined the meeting, which was jointly organized by the Department of Local Governance and Disaster Management of the Ministry of Home Affairs in Bhutan and the United Nations Satellite Center (UNOSAT) from the United Nations Institute for Training and Research (UNITAR).

This first official meeting of experts and stakeholders under this project provided a platform to foster a shared vision for infrastructure resilience and a collaborative approach to address the pressing

challenges posed by natural hazards and climate change.

Recognizing the need for adequate policy and regulation frameworks for disaster risk reduction in the critical infrastructure sectors, the project's core objective is to embed resilience in decision-making and investments. The project is expected to increase awareness and understanding of infrastructure resilience, while also strengthening national capacity for risk-informed and inclusive infrastructure policy and planning.

In his address to the meeting participants, the Chief of the Disaster Prevention and Mitigation Division of DLGDM, Ministry of Home Affairs summed up the significance of such a project by saying that "the DLGDM is gearing towards ensuring that the critical infrastructures are protected and are disaster resilient, as well as ensuring that our vital systems can withstand the test of time and disaster events".

## Auditors Can Assess and Advance Their Zero Trust Model with New ISACA Audit Programs

For organizations that adopt a Zero Trust approach for their cybersecurity program—adhering to the principles of "never trust, always verify"—it is important to periodically review, test and adjust their model to ensure that all users have the least amount of access to perform their jobs in order to better protect assets and systems. A new audit program from ISACA supports IT auditors in assessing these controls and processes to ensure their Zero Trust models are effective.

A subpar Zero Trust program can lead to major impacts, such as unplanned costs associated with incident response, significant impact resulting from regulatory censure, missed performance targets, system downtime, loss of business-critical data and/or systems, and reputational damage.

ISACA's Zero Trust Audit Program guides auditors in examining the core focus areas that can reduce the impact of a cyberincident.

The program can be used to assess an organization's ability to secure itself based on Zero Trust policies and procedures, as well as to evaluate related controls and their effectiveness in reducing the likelihood of a cybersecurity incident. The program also hones in on shortcomings pertaining to personnel, processes, technologies and governance, as well as various types of operational risk that could have a reputational impact.

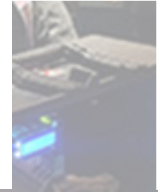




**critical  
infrastructure**  
PROTECTION AND  
RESILIENCE EUROPE



**12<sup>th</sup>-14<sup>th</sup> NOV 2024**  
**Madrid, Spain**  
[www.cipre-expo.com](http://www.cipre-expo.com)



## CALL FOR PAPERS

Deadline 31st March 2024

### Securing the Inter-Connected Society

The premier event for the critical infrastructure protection and resilience community.

The CIPRE Conference Committee are currently accepting abstracts for consideration for inclusion in the 2024 conference agenda.

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

The conference will look at the developing themes and challenges facing the industry, including the importance of the updated NIS2 Directive and Directive on the Resilience of Critical Entities and the obligations of CI owner/operators and agencies, as well as create a better understanding of the issues and the threats, helping to facilitate the work to develop frameworks, good risk management, strategic planning and implementation.

Join us in Madrid, Spain for the the 9th Critical Infrastructure Protection and Resilience Europe discussion on securing Europe's critical infrastructure.

Submit your abstract at [www.cipre-expo.com](http://www.cipre-expo.com)

**Leading the debate for securing  
Europe's critical infrastructure**

Co-Hosted by:

Media Partners:



To discuss sponsorship opportunities contact:

Paul Gloc

(Rest of World)

E: [paulg@torchmarketing.co.uk](mailto:paulg@torchmarketing.co.uk)

T: +44 (0) 7786 270 820

Sam Most

(Rest of World)

E: [samm@torchmarketing.co.uk](mailto:samm@torchmarketing.co.uk)

T: +44 (0) 208 123 7909

Jina Lawrence

(Rest of World)

E: [jinal@torchmarketing.co.uk](mailto:jinal@torchmarketing.co.uk)

T: +44 (0) 7958 234 750

Ray Beauchamp

(Americas)

E: [rayb@torchmarketing.co.uk](mailto:rayb@torchmarketing.co.uk)

T: +1-408-921-2932





## Protection of the EU's Critical Infrastructure: Evaluation of new legal instruments



By Robert Mikac, Security expert and Associate Professor, Faculty of political science at the University of Zagreb

Critical infrastructure is the essential objects and systems that underpin the functioning of a modern states, societies, and all kind of business. It includes entities from a sectors such as energy, transport, water, healthcare, telecommunications, and others. Disruptions to critical infrastructure can have a severe impact on national security, public safety, and economic activity.

In recent years, there has been a



Robert Mikac, Assistant Professor, Faculty of political science at the University of Zagreb

growing recognition of the need to strengthen the protection of critical infrastructure against a wide range of threats, including terrorist attacks, natural disasters, and cyber-attacks. In response to these threats, the European Union (EU) recently has adopted several new legal instruments to enhance the resilience and protection of critical infrastructure. The most significant among them are Directive (EU) 2022/2557 of the European

Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (hereinafter: CER Directive), and Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (hereinafter: NIS2 Directive). Both directives were passed at the end of 2022, and one year period after passing is the right time to evaluate them.

### The CER Directive

The CER Directive succeeded the Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (hereinafter: Council Directive 2008/114/EC), based on the European Commission's comprehensive evaluation study on the scope of the Council Directive 2008/114/EC, which has shown the need for upgraded and expanded scope. According to the 2019 Evaluation study of Council Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection ten years after entering into force: "the Directive appears today to have partial to limited relevance, notably in view of recent technological, economic, social, policy/political and environmental developments and current challenges"; the Member States (MS) adopted a variety of approaches in



transposing the Directive in their national legislation; the MS have different starting points and approaches towards the identification of potential European critical infrastructure; each MS adopted their own interpretations of what needed to be done regarding the Operator security plan and this has led to the adoption of different criteria for use in assessing risks for each MS; the MS very differently applied the requirements that the Security Liaison Office should satisfy; regarding the reporting of MS to the Commission, the procedure was established, however, it suffered from insufficiently high-quality use of the collected information by the Commission, and the Commission "has not systematically provided feedback on these reports, nor has it worked to synthesise the situational pictures at the MS level in order to create a pan-EU assessment of critical infrastructure vulnerability".

The CER Directive was adopted to eliminate those weaknesses and has repeatedly upgraded the scope and area of strengthening the resilience and protection of

critical infrastructure through various measures and activities. The key differences compared to the Council Directive 2008/114/EC are the following: Scope and coverage (CER Directive expands the scope to include all critical entities that provide essential services in 11 sectors, while Council Directive 2008/114/EC focuses exclusively on the energy and transport sector); Risk assessment approach (CER Directive encourages a more holistic, multi-dimensional approach that considers both physical and cyber threats, while Council Directive 2008/114/EC emphasizes a top-down, risk-based approach to critical infrastructure protection); Incident response and recovery mechanisms (CER Directive emphasizes the need for robust incident response and recovery plans to ensure continuity of critical services, while Council Directive 2008/114/EC provides limited guidance on incident response and recovery); Information sharing and cooperation (CER Directive strengthens requirements by establishing a centralized information-sharing platform (a Critical Entities Resilience Group is



hereby established) and promoting the exchange of best practices and lessons learned); Review and update mechanism (CER Directive mandates the establishment of a review mechanism to ensure that the Directive remains relevant and effective considering changing threat landscapes and technological advancements, while Council Directive 2008/114/EC does not explicitly provide for a regular review and update process).

Additionally, Council Directive 2008/114/EC was focused on the area of security, while CER Directive focuses on the internal market. Also, Council Directive 2008/114/EC focused on critical infrastructure, meanwhile CER Directive on critical entities that provide critical services where the critical infrastructure is needed to provide those critical services. Overall, the CER Directive provides a framework for physical and cyber resilience and protection of providers of critical services. Critical entities are those that provide basic services which are essential for maintaining important social functions, economic activities, public health, and environmental safety.

### The NIS 2 Directive

As in the previous case and for the same reasons, the NIS 2 Directive succeeded the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (hereinafter: NIS 1 Directive). Once again, the European Commission conducted a comprehensive evaluation study on the scope of the NIS 1 Directive. According to the 2020 Commission Staff Working Document Impact Assessment Report Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 certain weaknesses of the NIS 1 Directive are listed: the NIS 1 Directive falling short of ensuring a fully engaging, coherent and proactive setting that could guarantee an effective take of shared responsibilities and trust among all relevant authorities and businesses; the NIS 1 Directive revealed inherent weaknesses and gaps that

make it incapable of addressing contemporaneous and emerging cybersecurity challenges; the lack of clarity on the NIS 1 scope; the insufficient consideration of the increasing interconnectivity and interdependencies within EU economies and societies; the lack of alignment of security requirements and reporting obligations; the lack of effective incentives for information sharing or operational cooperation among relevant authorities; the difference in treatment of comparable businesses across MS and sectors; the NIS 1 Directive was not covering all sectors providing key services to economy and society. In order to address the above reasons, it was necessary to adopt a new and updated directive.

The NIS 2 Directive was adopted to eliminate weaknesses observed during the evaluation study. The main differences between NIS 2 Directive and NIS 1 Directive are following: Scope and coverage (NIS 2 encompasses a considerably larger scope than NIS 1, incorporating numerous new categories of entities, like government bodies, and placing a greater emphasis on digital infrastructure and ICT services, and expands from 7 operator of essential services sectors and 3 digital service providers categories to the 11 sectors of high criticality and 7 other critical sectors); MS obligations (NIS 2 more explicitly elaborates the requirements for MS' national cybersecurity strategies); Incident management and response (NIS 2 add the more efficient obligation of ensuring national large-scale incident management and response); Reporting obligation



(under NIS 2 reporting obligation has been tightened); International coordination (NIS 2 puts more focus on enforcing effective coordination between MS); Information sharing (under NIS 2 information sharing is more strongly encouraged); Supervision and enforcement (under NIS 2 supervision and enforcement have been tightened).

The NIS 2 Directive represent a significant piece of legislation that aims to improve the cybersecurity of the EU. The Directive aims to remove wide divergences among MS by setting out minimum rules regarding the functioning of a coordinated regulatory framework, by laying down mechanisms for effective cooperation among the responsible authorities in each MS, by updating the list of sectors and activities subject to cybersecurity obligations and by providing effective remedies and enforcement measures which are key to the effective enforcement of those obligations. The Directive contains stricter provisions on obligations of MS, essential and important entities, EU institutions and emphasizes the need for a more efficient cooperation. It also sets out the baseline for cybersecurity risk-management measures, and reporting obligations across the sectors that fall within its scope. The NIS 2 Directive extends the scope of implementation to new sectors and new stakeholders, strengthens supervision through sanctions and brings about a better and more efficient cooperation between MS. Instead of operators of essential services and digital service providers (from the NIS 1 Directive), the NIS 2 Directive introduces the categories of essential and important entities.



### Links between the two directives

Both directives boost the upgraded foundations of physical and cyber security, ensuring a resilient economy and society of each MS and the EU as a whole. Both directives contain many mutual references, describe how MS should apply them in coordination and cooperation between the bodies working on their implementation and explain how to avoid an administrative burden beyond that which is necessary to achieve the objectives of both directives. Among other things, they envisage the interlinkages between cybersecurity and the physical security, a coherent approach between these two directives. It is especially important to single out the provision stipulating that the entities identified as critical entities under the CER Directive should be considered to be essential entities under the NIS 2 Directive.

Furthermore, it is said that each MS should ensure that its national cybersecurity strategy provides a policy framework for enhanced coordination within that MS ensures between its competent authorities

(under both directives) information sharing about risks, cyber threats, and incidents as well as on non-cyber risks, threats and incidents, and the exercise of supervisory tasks.

All this strongly implies joint implementation of provisions from both directives, development of common characteristics in strengthening resilience and protection, but also brings challenges of common risks that can translate from one to the other normative area.

As both directives are very similar, the question arises whether one comprehensive directive could be created that would cover all the above? Or the above will happen in the next revision of both directives?

### Potential weaknesses

Both directives have some potential weaknesses that could limit its effectiveness.

First, the language of the directives is quite complex and contains a lot of technical detail. It will make it difficult to all stakeholders to understand and timely implement all the necessary obligations.



Second, the next example refers to a quite flexible approach to the adoption of a certain number of implementing acts, based on the provision that 'the Commission may' adopt them. In the CER Directive uses the phrase 'the Commission may' was used twice (in the first case, the possibility of inviting experts from the European Parliament to attend meetings of the Critical Entities Resilience Group, and in the second, to adopt implementing acts laying down procedural arrangements necessary for the functioning of the Critical Entities Resilience Group). In the NIS 2 Directive was used more time (regarding: implementing acts laying down procedural arrangements necessary for the functioning of the Cooperation Group; implementing acts laying down the technical and the methodological requirements, as well as sectoral requirements, as necessary, of the measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents

on recipients of their services and on other services; implementing acts further specifying the type of information, the format and the procedure of a notification which will ensure that essential and important entities notify about any incident that has a significant impact on the provision of their services; a candidate a European cybersecurity certification scheme regarding to use certain certified ICT products, ICT services and ICT processes).

Third, in both directives was avoid the definition of 'crisis' and in-depth elaboration of crisis management escalation procedures. In case of CER Directive, this has been left completely in the hands of the MS, which should develop critical entities resilience measures to ensure the implementation of risk and crisis management procedures and protocols and alert routines, but are required to inform the Commission in the event of an incident that has or might have a significant impact on the continuity of the provision of critical services for six or more MS. In the NIS 2 case, the MS are responsible for

and committed to cooperation within their national framework, and at the EU level via the CSIRTs network, the Cooperation Group, and the European cyber crisis liaison organisation network (EU-CyCLONe), whereby the Commission has its representative in the Cooperation Group, and an observer in the CSIRTs network, and the EU-CyCLONe. This kind of approach does not ensure a clear explanation of the term 'crisis' and/or 'cyber crisis' and laying down the escalation procedure in the event of a crisis / cyber crisis what brings a serious challenge for the implementation of the directives and efficient crisis management at the level of MS and at the EU level.

Fourth, both directives list too many sectors, subsectors and categories on the basis of which it is possible to identify and designate critical entities (according to the CER Directive) and essential and important entities (according to the NIS 2 Directive). This feels like an alibi solution, where too much room has been left for different interpretations and it is highly probable that too many operators of various facilities, network and/or systems will be declared critical entities, and essential and important entities, and which will lead to challenges in implementation compared to the Council Directive 2008/114/EC and NIS 1 Directive.

Fifth, the last challenge refers to the lack of procedural measures related to critical entities built and/or largely managed by EU institutions, whose critical services are used by all MS. These are critical entities of considerable strategic importance such as for example Eurocontrol, as a pan-

European, civil-military organisation dedicated to supporting European aviation; Galileo, as a global navigation satellite system; MeteoAlarm, as a European alerting system for extreme weather; etc.

### Conclusion

The new legal instruments (the CER Directive and the NIS 2 Directive) represent a significant normative improvement and will surely contribute to more efficient

measures to strengthen resilience and protection of the critical infrastructure, better cooperation and communication between numerous stakeholders and less exposure and damage because of incidents and irregularities in the functioning of various parts of the system. However, as no perfect regulation exists, the CER Directive and the NIS 2 Directive have certain potential weaknesses. Some of them are highlighted here.

## Russian Cyber Actors are Exploiting a Known Vulnerability with Worldwide Impact

To raise awareness and help organizations identify, protect, and mitigate this malicious activity, the authoring agencies have jointly released the Cybersecurity Advisory (CSA), "Russian Foreign Intelligence Service (SVR) Exploiting JetBrains TeamCity CVE Globally."

The CSA details the tactics, techniques, and procedures (TTPs) employed by the SVR actors, technical details of their operation, indicators of compromise (IOCs), and mitigation recommendations for network defenders.

The U.S. Cybersecurity & Infrastructure Security Agency (CISA), the Polish Military Counterintelligence Service (SKW), CERT Polska (CERT.PL), and the United Kingdom's National Cyber Security Centre (NCSC-UK) collaborated with NSA and the FBI to assess the SVR cyber actors' recent malicious activities.

The SVR cyber actors, who are also



known as Advanced Persistent Threat 29 (APT 29), the Dukes, CozyBear, and NOBELIUM/Midnight Blizzard, have been targeting Internet-connected JetBrains TeamCity servers globally as early as September 2023. Victims identified in the report include companies that provide software for billing, medical devices, customer care, employee monitoring, financial management, marketing, sales, and video games, as well as hosting companies, tool manufacturers, small and large IT companies, and an energy

trade association.

The CSA notes that SVR actors exploit a known vulnerability, CVE-2023-42793, to gain initial access to the TeamCity servers and then perform malicious activities, such as escalating privileges, moving laterally, deploying additional backdoors, and taking other steps to ensure persistent, long-term access to the compromised network

environments.

According to the CSA, software developers use TeamCity servers to manage and automate software development, compilation, testing, and releasing. Access to a TeamCity server can provide malicious actors with access to source code, signing certificates, and the ability to subvert software compilation and deployment processes and conduct malicious supply chain operations.



## Advancing Puerto Rico's Grid Recovery and Modernization

Natural disasters in recent memory have posed significant challenges to Puerto Rico's electrical grid and the more than three million residents it serves. In September 2017, Hurricanes Irma and Maria caused most of the transmission and distribution system in Puerto Rico to collapse, leading to one of the longest blackouts in U.S. history and leaving residents in some parts of the territory without electricity for almost a year. Merely five years later, Hurricane Fiona again knocked out 100% of the grid for as long as four weeks in parts of Puerto Rico, underscoring the critical need for urgent electrical grid modernization in the region.

In response to the crisis reignited by Hurricane Fiona, President Biden tapped Energy Secretary Jennifer Granholm to create the Department of Energy's (DOE) Puerto Rico Grid Recovery and Modernization Team. Housed within the Grid Deployment Office (GDO) and led by Agustín Carbó, this team works across federal government agencies – including but not limited to the Departments of Housing and Urban Development, Commerce, and Agriculture; Federal Emergency Management Agency (FEMA); and Environmental Protection Agency – to cut through bureaucratic red tape and access federal funding, coordinate technical assistance, and support current rebuilding activities in an expeditious and strategic manner. The team also works closely with government leadership and energy stakeholders in Puerto Rico to speed up the deployment of critical infrastructure and provide the island with clean,



reliable, and affordable power.

Since Hurricane Fiona, the Puerto Rico Grid Recovery and Modernization Team has facilitated multiple visits by Secretary Granholm to the region and made remarkable progress in local energy resilience. In December 2022, Congress approved \$1 billion to establish the Puerto Rico Energy Resilience Fund (PR-ERF) to support the region's most vulnerable and disadvantaged households and communities. In November 2023, the U.S. Department of Energy (DOE) announced its selectees from a \$450 million Funding Opportunity Announcement under the (PR-ERF). The funding will incentivize the installation of up to 40,000 residential solar photovoltaic (PV) and battery storage systems for vulnerable single-family households in Puerto Rico. DOE also announced 16 local community organizations as selectees for the Solar Ambassador Prize, an opportunity to assist DOE in identifying and assisting with intake processing of qualifying households for these critical residential solar systems. DOE anticipates the first installations to begin in spring of 2024.

In the coming weeks, DOE will also announce the results of the Puerto

Rico Grid Resilience and Transitions to 100% Renewable Energy Study (PR100), which is defining pathways for Puerto Rico to be entirely powered by clean energy by 2050. This goal was established by the Puerto Rico legislature in 2019 through its passage of the Puerto Rico Energy Public Policy Act (Act 17), and DOE is leveraging the experts in six

of its national laboratories to ensure energy system resilience against extreme weather events and advance energy justice locally.

DOE has also made historic investments in Puerto Rican energy resilience through a \$3 Billion Partial Loan Guarantee to Sunnova's Project Hestia, with 20% of all loans to homeowners in Puerto Rico; awarding a \$7.4 million Grid Resilience Formula Grant to the government of Puerto Rico; investing in critical resilience hubs, and sponsoring technical assistance for local energy resilience projects through the Communities LEAP program.

DOE has also continued to deploy its national laboratories to provide technical assistance to the Puerto Rican government and utility, providing grid managers with the tools, training, and modeling to improve the operation and planning of the electric system. These projects have ranged from supporting the development of a request for proposals for a critical microgrid at San Juan's Centro Médico, to developing modeling tools to help grid operators better plan electricity recovery operations after natural disasters.

**ECHODYNE**

**AXIS**<sup>®</sup>  
COMMUNICATIONS

**Empowering resilient security:**  
Detecting drones with radar and cameras

**You're invited!**

**Demo & Drinks**

Live drone detection demo

**Wednesday**

**March 13 at 5:30pm**

**L'Auberge Hotel & Casino, Lake Charles, LA**



## CIP: coming of age, facing new challenges



By Albert Nieuwenhuijs and Ignas Melman, TNO Netherlands

The term 'critical infrastructure' and the active protection of it (CIP), was introduced almost 25 years ago. We have come a long way since then; even if current policies and techniques might not be perfect, and implementation varies between countries, CIP is now a mandatory element in national and EU-wide policy.

Although this is an important step, we must remain vigilant. The world changes, both infrastructure and threats evolve; to stay effective,

our protection has to adapt. In this article we identify some trends that challenge the current paradigm of CI protection. To deal with these changes, we need to find ways to address them.

These new ways will require new analysis and protection techniques, more emphasis on resilience, a closer integration of aspects like cyber and hybrid threats, and more and better coordination of infrastructure protection between parties that up to now, have been

working in silos.

### **A brief overview of the development of critical infrastructure protection**

The term 'critical infrastructure' has been with us for some time now. Although lists of national assets deemed to be most critical to defend in times of conflict have been around longer, the term 'critical infrastructure' (CI) was coined as early as 1996 in the USA with the definition of eight





sectors (Bill Clinton, Executive Order 13010: Critical Infrastructure Protection, 1996). Two years later, this was followed by a presidential decision directive to develop a capacity to protect CI. (Bill Clinton, Presidential Decision Directive 63, 1998).

Two years later, the Y2K problem (Wikipedia, sd) served as an eye-opener worldwide: suddenly there was a worldwide example of one vulnerability which could affect many systems over a wide array of sectors, posing a potential threat to the well-functioning of the nation. This made nations worldwide aware of the need to discover their own CIs and their possible vulnerabilities. Several nations followed up on this need and started national programmes, identifying the fact that indeed, critical infrastructure was a concrete subject of investigation that warranted constant protection, not only in times of conflict.

These national initiatives yielded concrete results and identified both national and cross-national critical sectors and raised awareness on their vulnerabilities. The results gained in national initiatives and the emerging awareness about the

need for a coordinated approach led to the European Program for Critical Infrastructure Protection (EPCIP) in 2006. This program and its various successors and spin-offs (EU, 2019), with its arguable successes and compromises, have resulted in CI protection (CIP) being a mandatory element of national government in all EU countries (EU, 2008) and boosted the knowledge of and experience with CIP.

Both the US and EU initiatives have evolved over the years, updating the list of CI sectors to be considered, the requirements for protection of those sectors and increasing the emphasis on resilience, not just protection (Lazari, 2014) (Perelman, 2007) (Setola, Luijff, & Theocharidou, 2016). Although the implementation of the EU directive varies per EU member state, one thing that has remained constant over all those years, is the high-level approach taken in these programs : identifying critical sectors, analysing their vulnerabilities and (inter) dependencies, and identifying measures to mitigate and deal with unacceptable identified risks (Lindström, 2009) (TNO, 2011). The premise is that this approach is an

effective way to protect CIs (and consequently society as a whole) from harm. As we are gaining ever more experience with this approach and are improving it, its challenges become apparent, specifically in the light of changing and emerging threats.

Trends that challenge the current CIP approach

A number of trends can be identified that challenge the effectiveness of this approach in CIP. We will try to list these trends below and elaborate on why they pose a challenge.

#### Increased digitization

In a constant search of increased productivity, digitization and automation offer unparalleled opportunities for society. But as always, where there is a gain, there is usually a loss as well. In this case, some of the side effects of increased digitization and automation affect the effectiveness of the current CIP strategy.

Increase in automation and autonomy at the cost of intelligence and flexibility

Digitization allows for increasing productivity by increasing autonomy of parts of the CI. Examples of increased automation and autonomy are: replacing a human bridgeman with a camera and remote-control system, autonomous measuring and control systems, centralized control rooms and electronic access systems. The amount of monitoring and control that is shifted from direct human involvement to a remotely controlled or automated operation varies with each example, but in all of these examples there is a certain loss of intelligence and flexibility: a

camera will not recognize a street-race in the making that is about to cross the bridge, a measure and control system will not be able to quickly self-repair small technical malfunctions, a centralized control room will reduce the number of locations monitored at any one time and increase response time and an electronic access system will not be able to tell if a server park manager has been under duress lately.

These are just a few examples that illustrate the loss of intelligence and flexibility due to automation and increased autonomy. Of course, there are examples as well where the opposite is true, in which case automation and algorithms are used to enhance intelligence and flexibility. The point here is that if this aspect is not considered before automating processes, chances are that it will result in a loss of intelligence and flexibility. The afore mentioned examples span a loss of detection, prediction, reasoning, decision and action capabilities. Programmed automation types are particularly strong in gathering data and rule-based decision making, which requires the decomposition, formalization and capturing of rules of the task within strictly defined parameters (for example: (Shi, Lee, & Kuruku, 2008)). This step by its nature disregards additional capabilities and tasks of a human operator not directly indispensable to the basic task, such as predicting a dangerous situation is developing (the street race) or detecting emotional instability (door guard instead of electronic access system). More artificial intelligence-based automation could potentially (to some extent) overcome this limitation, but some higher

reasoning capabilities currently still pose a challenge (Hechler, Oberhofer, & Schaeck, 2020).

Another effect of continuing automation and autonomy is the reduction of available human resources. Infrastructures are now controlled in central control rooms instead of on-site, so there are significantly less employees necessary to operate the same number of infrastructures. Consequently, the reaction time to an incident is longer, as it takes time to send employees to the site of the incident for repair activities. In the case of a large-scale incident encompassing multiple areas, there might not even be enough employees available to respond to the incident adequately, as they do not have the numbers to spread out to the incident areas. Automation thus leads to a reduction of human capacity, which leads to a decrease of flexibility and fall-back options.

Increase in productivity at the cost of resilience and flexibility

Digitization as an enabler for increased productivity also has a second side effect: the cutting of stocks and play in the supply and production chain. The economic benefits are clear (Marshall, 2020): smaller stocks, less use of resources and less waiting time lead to higher efficiency, provided that the process is predictable. Digitization facilitates this process in two ways:

- It can make the process more predictable (by better logistics, process control, communication) and
- It allows for optimization to span organizations in the production chain (by enhanced communication and linking processes).

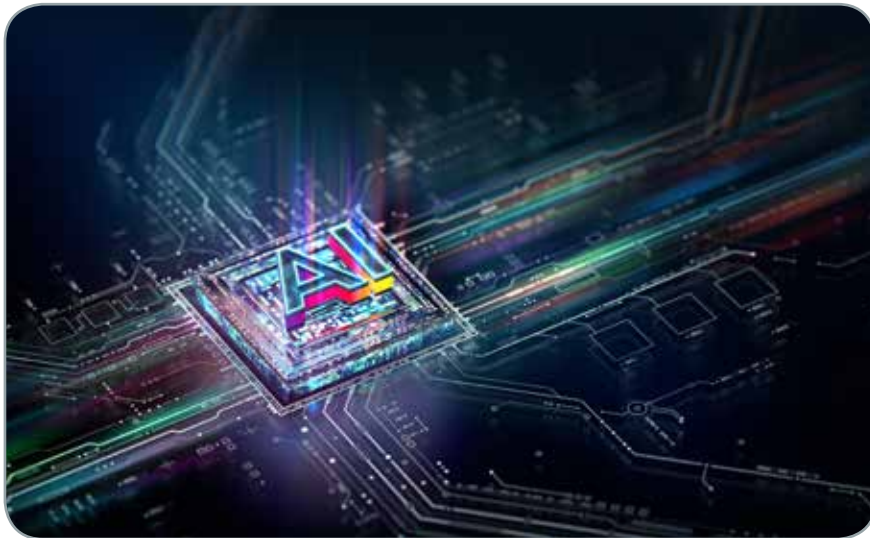
Unfortunately, both mechanisms can decrease the resilience of CI organisations:

- By relying more on the predictability of a process, it will become more vulnerable to unforeseen disruptions;
- By linking processes across organization, the vulnerability for disruption by processes outside your own organization is enhanced. C. Perrow argued as early as 1984 that complexity and tightly coupled systems make these systems inherently vulnerable to disruptions. Because technology is tightly coupled, the impact of the disruption can spread through the system, which may ultimately escalate into a system accident (Perrow, 1984).

This shows that we need to change the way we deal with the protection of our infrastructures, from the current practice to build infrastructures and adapt processes in order to optimize efficiency and deal with the consequences later, towards integrating protection and resilience into the fabric of our design process. We call this 'resilience by design', an analogy for the term 'security by design'. Resilience needs to be included as a design parameter in the design of infrastructures, rather than implementing it as an afterthought.

Increased complexity and dynamics

Digitization facilitates creating complex CI structures on a sectoral, cross-sectoral and a cross-border level. These structures offer an increase in efficiency, but the resulting complexity poses an ever-higher challenge to the classic approach of CIP, as the increasing complexity will result in an increase of the time and effort needed to



map/assess these structures. At the current level of complexity, we already see that there are sectors where any effort at mapping them comprehensively (and the modeling required to do this) is outdated by the time it is finished (Mittal & Tolk, 2020) as the relations and dependencies within and between the infrastructures have a dynamic nature and change rapidly.

This is especially valid for the ICT landscape and the use of ICT in almost all CI sectors. Vulnerabilities and dependencies can be found on many levels within systems, such as software or hardware, but also within services, products or data. Because the ICT landscape develops and changes so quickly, it is a challenge to map the vulnerabilities and dependencies which are caused by these changes comprehensively.

Concluding, an ever-increasing effort is needed to sustain the current siloed approach of identifying and analysing critical sectors along with their vulnerabilities and interdependencies. The traditional methods are not scalable in the long run and therefore untenable for the future.

### Increased common risks

As our society evolves, we see increasing risks that are common to several infrastructures. These risks are increasing both on account of increasing common vulnerabilities and common threats. These common risks can be categorized as follows:

- Shared structures, suppliers and services;
- Homogeneous organisational structures;
- Common threats;
- Climate change.

Shared structures, suppliers and services, (such as ICT, software and supply chains) provide common vulnerabilities for all parties who depend on them. The Citrix vulnerability that was revealed at the end of 2019 (Positive Technologies, 2019) showed how many businesses depended on the product of a single supplier – and were not aware of it. Similarly, many CIs may be dependent on a small number of suppliers, products and services, without knowing exactly what the effects are (within their company, sector or country) if there is a malfunction in one of their supply chains.

Another increase in common vulnerabilities can be found in organizational structures. We see a trend where there is less diversity in organizational structures, which may increase the chance of common points of failure. A successful attempt of malicious activity in one company will probably have a high likelihood to succeed in another company as well. An example is that many companies have a function titled Chief Financial Officer (CFO). When companies all have a CFO with a similar job description, it makes them more vulnerable to social engineering attempts by cybercriminals or state actors: it is easier to combine these common structures with publicly available information (i.e., annually published reports with figures) to fill in the blanks about a specific company, than it would be when companies had unique organizational structures.

While common vulnerabilities increase, we also see an increase in the common threats that CI operators face. These common vulnerabilities are an attractive target for state actors and cybercriminals, since they are able to cause a high impact by attacking only one target.

Climate change also forms a cross-border common-cause threat. In the last decades, events like wildfires, hurricanes and floods have disrupted or destroyed CIs. Extreme weather as a consequence of climate change will become a more urgent problem as incidents in this category increase in frequency, intensity and impact. (Shakou, Wybo, Reniers, & Boustras, 2019)



In a siloed approach, these risks might not be rated high enough to necessitate mitigation in any single risk assessment. However, these risks have the potential to cripple many infrastructures at once, impacting society in a way that is currently not taken into consideration. As long as siloed risk analysis is the norm, we will keep underestimating these types of risk.

#### Addressing these new challenges

We addressed some trends that present a challenge to a siloed approach in CIP. As these trends are not likely to turn around in the foreseeable future, we need to take action now. While it is unlikely for a 'silver bullet' solution to exist that overcomes all identified weaknesses, we can identify some aspects that a possible solution is likely to encompass.

A first step is to take local resilience into account when enhancing processes: digitization and automation offer great possibilities not only for increase of productivity, but also for increasing resilience. They can be used for smart management of sharing distributed / redundant resources, using multiple suppliers or supply routes, or facilitating quick changes in production locations and processes. All of these options require complex control and management, which digitization and automation techniques excel in.

Secondly, we need to give more attention for getting a handle on dealing with the ever-growing complexity of our infrastructure and finding a way to effectively identify risks before dynamics in the system or the environment has rendered the analysis obsolete.

Lastly, a mechanism is needed to identify relevant common threats and vulnerabilities and how to mitigate them and address them at a company, sector or nation transcending level, whichever is most appropriate for the specific threat. This will likely have to include some form of high-level decision mechanism to enable mitigation measures that are for the good of the whole, but can go at the cost of individual companies, sectors or nations. An example would be the ban on paying ransom for cyberattacks: we know that paying leads to more attacks, but an individual company has other, more pressing problems when hacked. If no reasonable alternative to paying ransom is created, this problem will keep growing and require a solution overarching the problem holders. As of today, no entity that is willing and able to create such a solution has been found.

#### Conclusion

Increasing digitization and automation of our society have consequences for the way our critical infrastructure can and should be protected. The conventional silo approach in which the vulnerabilities and dependencies of individual sectors or individual threat types are studied no longer suffice to sufficiently protect our critical infrastructure in the light of digital and hybrid threats and ever-more entwined infrastructure. A paradigm shift in our method of protecting critical infrastructure is needed if we want to keep our critical infrastructure safe.

#### About the authors:

*Albert Nieuwenhuijs is a senior researcher at TNO, the Netherlands Organisation for Applied Scientific Research. His main areas of scientific research include Critical Infrastructure Protection and communal safety and security.*

*Ignas Melman is a researcher at TNO, the Netherlands Organisation for Applied Scientific Research. His main areas of scientific research include Critical Infrastructure Protection and cyber security and cyber crime.*



## Game-Changing Cyber Defender Emerges SEAS Safeguards Critical Infrastructure

For the Critical Infrastructure Sector, Traditional Firewalls as a single line of defense are a Distant Memory. Introducing SEAS: a revolutionary cyber sentinel rewriting the playbook on data security. This transformative technology, validated by the US Navy, goes beyond mere defense – it's a paradigm shift in securing communications.

SEAS is not your grandparents' cybersecurity. Forget patching firewalls and scrambling after breaches. These plug-and-play "smart" modules, stationed at network endpoints, become invisible guardians, autonomously detecting and thwarting attacks in real-time.

No red tape, no incident response teams – just seamless protection, even for legacy systems. Here's why SEAS is a game-changer:

1. Zero-Trust Hero: Unlike perimeter-based defenses, SEAS secures every endpoint, from cutting-edge servers to dusty PLCs.
2. Quantum-Proof Champion: Forget 2023's Warnings – SEAS's symmetric encryption makes Quantum Attackers cringe!
3. Real-Time Guardian: No more waiting for breaches. SEAS instantly identifies and blocks attacks, providing real-time insights and analytics.
4. Easy Breezy Management: The SEAS Management Console simplifies everything, from user permissions to network segmentation.
5. But SEAS's power lies in its core:
  - a. Patented Trust Algorithm: Every network message is rigorously authenticated and validated, leaving no room for deception.
  - b. Operational Technology Champion: SCADA, DCS, PLCs – whatever your OT backbone, SEAS secures it, paving the way for safe IT/OT convergence.



The Critical Infrastructure Sector is under siege. But with SEAS, the tides are turning. This plug-and-play powerhouse offers an immediate, cost-effective way to future-proof your defenses.

**Don't wait for the next cyberquake. Deploy SEAS and become the master of your digital domain.**

SEAS LLC, 3201 Stellhorn Road, Suite D127, Fort Wayne, IN 46815.

Business Development Phone: 260-407-1755 / Email: [info@SEAS-US.org](mailto:info@SEAS-US.org)

[www.seas-us.org](http://www.seas-us.org)

# Enhancing Security Through Integration: The Crucial Role of Integrating Physical Security Systems



Dave Peters is a Product Marketing Director with Everbridge. Dave has 20 years of experience in the physical security space with a focus on solution design and integration.

The past 20 years have seen extraordinary advancements in physical security technology. What started with the transition of analog to digital of common physical security systems such as CCTV, access control, and intrusion, has further evolved with the introduction of advanced technologies, such as video analytics, facial detection, and license plate recognition. We are now in an era where artificial intelligence and machine learning are providing another new set of



Dave Peters, Product Marketing Director, Everbridge

tools to identify and respond to threats. These tool sets provide security operations with an immense amount of data and actions. They also introduce the challenge of how to best utilize and manage these tools.

Research has shown that 90% of organizations are using security systems and devices from multiple manufacturers, with a large number using technology from 10+ different manufacturers.



This results in a disparate set of applications, alerts, actions, and data that creates inefficiencies throughout the operations center. Operators are tasked with analyzing and responding to ever increasing alarms and events generated from these independent systems. Interacting with multiple systems is often needed as part of the response. This requires the operator to be proficient with all systems involved, know the appropriate actions to take in their proper order when an event occurs, and gather all supporting data after the event to support analysis and reporting.

The challenge is further exasperated when a new system is introduced. This may be a new technology that management believes will enhance security or meet compliance, or an additional manufacturer of an existing system. Through acquisition or phased obsolescence, organizations may find themselves with multiple systems, such as CCTV or access control, from multiple manufacturers.

Lack of interoperability between systems significantly impacts an organization's ability to respond to events quickly to keep their people, facilities, and assets safe and their organization running.

Organizations have options:

**Do nothing** – This will result in ever increasing information overload, risk of missing events, no consistency in response from operators, spiraling costs via additional operators and training, and data that continues to live in silos.

**Standardize** – Standardization of physical security systems can be very costly. There may be a significant capital investment in existing technologies. If choosing to standardize, the organization is then locked into the single vendor. This reduces negotiating power and



limits the ability to choose best-of-breed systems.

Integrate the disparate technologies – Integration of physical security systems to create a common interface for operators provides security operations with the capability to respond quicker and more consistently. Integration provides a unified system rather than independent entities. This interconnected approach ensures that information flows freely between components, providing a more comprehensive and real-time view of the security landscape.

One of the primary advantages of integrating physical security systems is the ability to achieve real-time awareness. By connecting surveillance cameras, access control systems, intrusion and other sensors, security personnel gain a comprehensive view of their environment. This integrated approach enables a proactive stance against potential threats, as security teams can monitor events in real-time and respond swiftly to emerging situations. This can be

further extended to operational systems such as building management and manufacturing systems, which generate their own events that may require security response.

Large operations centers may deal with hundreds, even thousands, of alarms and events from their security systems on any given day. The vast majority of these are trivial, but still need to be verified. Improving response times to the trivial can result in significant operational efficiencies. If an operator needs to interact with multiple non-connected systems to assess an event, it introduces delays. Now combine this with an operator's lack of training or understanding of all systems, multiplied by every alarm triggered throughout the day – to say the least, the operator's average time to handle an event will not be optimal. Presenting the operator who is handling the alarm with the appropriate contextual information, automatically and within the same interface, allows for a quick and accurate assessment and closure of

the event.

Many alarms and events managed by operators turn out to be nuisance or false alarms. Integration of systems allows for data and events to be correlated against each other. The integrated system can then limit alarms being presented to the operator unless one or more criteria is met. For example: an alert from a motion sensor in an intrusion system may not be presented as an alarm unless a second system in the area, such as CCTV or access control, also reports an event within a given timeframe. Providing validation from a second system prior to presenting the alarm to an operator can limit the number of false alarms an operator is required to handle. Additionally, correlated alarms can be combined into a single event, allowing operators to manage multiple alarms through a single action.

While handling the trivial may be the majority of an operator's workday, what happens when a major event occurs? Will the operator be able to efficiently assess, locate, and act? As part of the integrated approach to assessing and locating the event, providing the operator with the appropriate standard operating procedures (SOPs) to act and respond is vital. Many organizations store their SOPs separately from their security systems. This may be a shared drive on their network, or perhaps in a binder on a shelf. Digitizing these procedures and embedding them into your integrated security solution provides a multitude of advantages. Not only will it present the operator with the appropriate response plan to manage the event, but actions can also be automated through programmable steps or triggers that the system can take based upon operator input.

Let's use a perimeter intrusion as our example. The intrusion sensor sends an alert to the operations center. The handling operator is automatically presented with sensor data, appropriate CCTV cameras, map of the area, and the SOP. As the operator follows the SOP to assess the incident, they determine it is a critical event. Once determined, the integrated system can automatically trigger actions within other systems, to include creating a computer aided dispatch (CAD) request, lowering gates that may be open during business hours, and notifying the appropriate personnel via email or mass notification. These are actions that, when done manually, take valuable time away from the operator and their focus on the event, and may even be missed. The example above shows interaction with five or six systems. Some events may require even more. The speed of response is critical in situations where immediate action is required. Automated alerts and notifications provide security teams with timely information, allowing them to assess the situation rapidly and initiate appropriate responses. This proactive approach can make the difference between thwarting a security threat and experiencing a significant breach.

While achieving more efficient assessment and response to events is often the primary focus of security operations, having a comprehensive reporting tool is often overlooked. When dealing with disparate systems, each system creates its own set of data to include events, operator actions, and health of its components. Integration creates a single repository for this information that can then be analyzed at a macro level as well as refined to individual events, systems, areas, or locations. To generate an incident report for the perimeter

intrusion example described above, gathering all appropriate information from disparate systems is a time-consuming task that involves exporting all relevant data from each supporting system, and combining and formatting it into a single comprehensive report. Data may include CCTV video, access control logs, operator actions, and field responses. As part of an integrated solution, incident reports can be generated immediately upon resolution, with the relevant supporting data disseminated to the appropriate people. Reports from an integrated system can provide insight into every aspect of security operations. It can correlate data from all systems to report on most active sensors, response and handling time of operators, and what locations or regions are most active. Trends can be spotted, and operations improved through more efficient staffing, adjustment in subsystem configurations, and optimizing SOPs.

Many industries are subject to stringent regulatory requirements regarding security and surveillance. Integrated physical security systems facilitate compliance by providing a consolidated repository of data for auditing purposes. This not only simplifies the auditing process but also ensures that organizations can demonstrate adherence to regulatory standards. Compliance with industry regulations and standards is non-negotiable for organizations, as failure to meet these requirements can result in severe consequences, including legal repercussions and reputational damage. Integrated systems streamline the process of gathering and presenting data during audits, reducing the burden on security teams and ensuring a more thorough and accurate assessment of compliance.

While the integration of physical security systems offers numerous benefits, it is not without its challenges. Ensuring compatibility between disparate systems, addressing cybersecurity concerns, and providing adequate training for personnel are crucial considerations. Organizations must adopt a strategic approach to integration, collaborating with experienced vendors and prioritizing cybersecurity measures to maximize the effectiveness of integrated systems. Assignment of an internal project team that includes a dedicated project manager and stakeholders from security, IT and management teams will ensure that implementation stays on track and avoids delays and cost overruns. Integration projects that have failed or experienced significant delays are often not the fault of the technology itself, but rather poor planning during design and rollout. Full commitment to the success of the project is paramount.

The diverse landscape of physical security technologies can also pose challenges related to compatibility and interoperability. Integrating systems from different vendors or utilizing legacy systems may require additional efforts to ensure seamless communication and data sharing. Organizations should prioritize solutions that support open standards and APIs to facilitate smoother integration processes.

As physical security systems become more interconnected, the risk of cybersecurity threats increases. Protecting integrated systems from unauthorized access, data breaches, and other cyber threats is crucial. Implementing robust cybersecurity measures, including encryption, regular software updates, and access controls, is essential to safeguarding the integrity and confidentiality of sensitive security data.



The success of integrated physical security systems relies heavily on the competence and understanding of the personnel operating and managing these systems. Comprehensive training programs are critical to ensuring that security teams are proficient in utilizing the integrated platform effectively. This includes understanding how to interpret data, respond to alerts, and leverage the full capabilities of the integrated system. The integrated platform supports not only a single interface the security team can use to manage events, but can also be configured in a manner that best fits the organization's concept of operations.

The integration of physical security systems represents a paradigm shift in how organizations approach safeguarding their assets and people. By promoting real-time awareness, expediting response times, and aggregating data for reporting, integrated systems create a comprehensive and proactive security environment. As the threat landscape continues to evolve, the importance of a well-integrated and technologically advanced physical security infrastructure cannot be overstated. It is a cornerstone for organizations looking to stay ahead

of security challenges and protect what matters most.

The integration of physical security systems is not just a technological evolution but a strategic imperative for organizations seeking to fortify their defenses against an array of security threats. As technology continues to advance, the integration of physical security systems will remain a dynamic and ongoing process, demanding constant adaptation and improvement. Organizations that embrace this integration journey stand to benefit not only from enhanced security but also from the ability to make informed decisions based on comprehensive data analytics. As we navigate an increasingly complex security landscape, the integration of physical security systems is a proactive step toward a safer and more secure future.





Critical Infrastructure Protection & Resilience Europe (CIPRE) took place on 3rd-5th October 2023 in Prague, Czech Republic, co-hosted by the Ministry of Industry & Trade of the Czech Republic and the International Association of CIP Professionals (IACIPP) and supported by the Tomas Bata University in Zlin and Technical University of Ostrava.

We take a look at the success of the conference and exhibiton and some of its highlights reported by John Donlon, Chairman of CIPRE.

It gives me great pleasure to invite you to join us at the Critical Infrastructure Protection and Resilience North America (CIPRNA) conference in Lake Charles, Louisiana, for what will be 3 days of exciting and informative discussions on securing North America's critical infrastructure.

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

There is an exciting line up of topics and speakers, which can be viewed on the CIPRNA website. It is a very packed agenda, which will seek to explore the complexities and innovations in place around the protection and resilience of our Critical National Infrastructure and Information.

CIPRNA seeks to bring together leading stakeholders from industry, operators, agencies, academia and governments to provide detailed insights into current policy and practices and to collaborate on the efforts required to continually address the range of challenges faced across infrastructure sectors. The conference will look at developing on the theme of previous events, both here in the United States and across Europe, in helping to create a better understanding of international issues and in providing a way forward when developing future strategies and processes.

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

Our world continues to be unpredictable and is changing at an incredible pace. The challenges that have to be addressed, both natural and those that are human caused are increasing in complexity, frequency and magnitude and this is reflected across our critical infrastructure and information sectors.

Those infrastructure and information sectors, as we all know, provide the essential services that underpin our societies and are a significant contributor to economy security and health. The threats, vulnerabilities and consequences that they all face have evolved over time and are severely impacted by the onslaught of major global events.

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

The last year has seen a significant evolution in the cyber threat posed not least due to Russia's ongoing invasion of Ukraine. We also continue to see evidence of China state-affiliated cyber actors deploying sophisticated capability to pursue strategic objectives and while it is less sophisticated than Russia and China, Iran continues to use digital intrusions to achieve its objectives, including through theft and sabotage.

The availability and capability of emerging technology has a pivotal role within all of this. As Artificial Intelligence continues to advance and reshape the landscape of various industries, state actors will continue to develop its use in seeking to cause harm. However, it is also transforming the fields of security, risk and crisis management. It offers new approaches to handle complex security challenges, to enhance risk assessment models and revolutionises crisis management protocols.

The world is constantly changing as wars, geopolitics and climate change are adding further complexity in the security and resilience of our nations. As the pace of that change continues to accelerate so to must our efforts to deal with the range of challenges across the Physical, Cyber and Natural Disaster spectrums.

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

In seeking to address these issues there is a fantastic agenda lined up with the CIPRNA event in Lake Charles, with some excellent speakers covering a wide range of important topics and presenting their considered views on the way forward in protecting, securing and developing the resilience of our infrastructure and information internationally.

The conference is specifically designed to stimulate debate and as we have found at all of the events across North America and Europe, the active participation of all involved across the sessions adds real value in the development of new thinking.





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

This will be a most rewarding and enjoyable event and I hope to see you in Lake Charles.

John Donlon QPM FSyl

CIPRNA Chairman

Chairman - International Association of CIP Professionals



## Exhibitor Showcasing in the Expo:

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



**Pre-Register for your Expo Only Pass at just \$10**

**[www.ciprna-expo.com/onlinereg](http://www.ciprna-expo.com/onlinereg)**

(\$50 on-site registration)

\*Includes coffee





## A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

### Schedule of Events

#### Tuesday March 12<sup>th</sup>, 2024

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

1:00pm - Exhibition Opens

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

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

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

5:30pm - Networking Reception in Exhibition Hall

#### Wednesday March 13<sup>th</sup>, 2024

##### TRACK ONE

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

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

11:15am - 12:30pm - Session 3a: Communications Sector Symposium

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

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

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

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

##### TRACK TWO

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

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

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

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

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

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

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

#### Thursday March 14<sup>th</sup>, 2024

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

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

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

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

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

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

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

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

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

4.30pm - Expo Close

**Register online at [www.ciprna-expo.com/register](http://www.ciprna-expo.com/register)**





## *A Homeland Security Event For Securing Critical Infrastructure and Safer Cities*

### Why Attend?

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

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

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

For further information and details on how to register visit [www.ciprna-expo.com](http://www.ciprna-expo.com)

For conference or registration queries please contact:  
Ben Lane  
Event Director  
E: [benl@torchmarketing.co.uk](mailto:benl@torchmarketing.co.uk)

### Who Should Attend

Critical Infrastructure Protection and Resilience North America is for:

- Police and Security Agencies
- DHS, CISA, FEMA, TSA, DISA, GAO, NSA, NCTC, FBI and related emergency management, response and preparedness agencies
- Emergency Services
- National government agencies responsible for national security and emergency/contingency planning
- Local Government
- CEO/President/COO/VP of Operators of national infrastructure
- Security Directors/Managers of Operators of national infrastructure
- CISO of Operators of national infrastructure
- Facilities Managers – Nuclear, Power, Oil and Gas, Chemicals, Telecommunications, Banking and Financial, ISP's, water supply
- Information Managers
- Port Security Managers
- Airport Security Managers
- Transport Security Managers
- Event Security Managers
- Architects
- Civil Engineers
- NATO
- Military
- Border Officials/Coast Guard

***Join us in Lake Charles, LA for Critical Infrastructure Protection and Resilience North America and join the great debate on securing America's critical infrastructure.***

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



*A Homeland Security Event For Securing Critical Infrastructure and Safer Cities*

### Exhibition Opening Hours

Tuesday March 12th	1.00pm to 7.30pm
Wednesday March 13th	9.30am to 5.30pm
Thursday March 14th	9.30am to 4.30pm

### On-Site Registration Hours

Tuesday March 12th	8.00am to 6.00pm
Wednesday March 13th	8.30am to 5.00pm
Thursday March 14th	8.30am to 4.00pm

**REGISTER ONLINE AT [WWW.CIPRNA-EXPO.COM](http://WWW.CIPRNA-EXPO.COM)**

**Register Online Today at [www.ciprna-expo.com/register](http://www.ciprna-expo.com/register)**

### REGISTRATION

The Critical Infrastructure Protection & Resilience North America is open and ideal for members of federal government, emergency management agencies, emergency response and law enforcement or inter-governmental agencies, DHS, CISA, FEMA, TSA, DISA, GAO, NSA, NCTC, FBI, Fire, Police, INTERPOL, AMERIPOL and associated Agencies and members (public and official) involved in the management and protection of critical national infrastructure.

The Conference is a must attend for direct employees, CSO, CISO's and security, fire and safety personnel of critical infrastructure owner/operators.

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

### EARLY BIRD DISCOUNT - deadline February 12<sup>th</sup>, 2024

Register yourself and your colleagues as conference delegates by February 12th, 2024 and save with the Early Bird Discount. Registration details can be found at [www.ciprna-expo.com/register](http://www.ciprna-expo.com/register).

**REGISTER ONLINE TODAY AT [WWW.CIPRNA-EXPO.COM/REGISTER](http://WWW.CIPRNA-EXPO.COM/REGISTER)**

### Discounts for Members of Supporting Associations

If you are a member of one of the following trade associations, supporters of the Critical Infrastructure Protection & Resilience North America, then you can benefit from a special discount on standard rates:

- INFRAGARD LA
- The International Emergency Management Society (TIEMS)
- National Security & Resilience Consortium (NS&RC)
- International Association of CIP Professionals (IACIPP)
- International Security Industry Organization (ISIO)
- International Association of Certified ISAQs (IACI)

**Check the Registration Information at [www.ciprna-expo.com/registration-fees](http://www.ciprna-expo.com/registration-fees)**





## *A Homeland Security Event For Securing Critical Infrastructure and Safer Cities*

### Site Visit

#### **CITGO Lake Charles Refinery**

**Tuesday 12th March – 8.30am-12.30pm**

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

**Book your place online at [www.ciprna-expo.com/register](http://www.ciprna-expo.com/register)**



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

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

#### **Lake Charles Refinery**

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

#### **About CITGO**

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

petrochemicals, and other industrial products.

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

- Short-term immediate assistance to support local partners working on recovery efforts
- Long-term assistance to repair homes, rebuild communities and get them back to normal
- Equipment for first responders and community organizations designed to prepare for and accelerate recovery.





*A Homeland Security Event For Securing Critical Infrastructure and Safer Cities*

**Tuesday March 12<sup>th</sup>**

## Conference Programme

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

Chair: John Donlon QPM, FSI

*International adviser on security intelligence*

Representative for Congressman Clay Higgins

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

Senior Representative, Governors Office of Homeland Security & Emergency Preparedness

Mayor Nic Hunter, Mayor of lake Charles

---

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

---

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

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

*How should the CI community build situational awareness to mitigate the cascading effect across infrastructures.*

Chair: John Donlon QPM, FSI

Adam Stahl, Chief of Staff Corporate Security, AVANGRID

Cameron Dicker, Director of Global Business Resilience, FS-ISAC

Chris Anderson, Co-Chair, Comm-ISAC

Anna Ballance, Sr. Advisor, Industry Policy Coordination, E-ISAC

**Critical Infrastructure Dependency Analysis** - National Laboratory Research and Development Advancements -

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

---

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

---

*\*invited*







## A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

**Wednesday March 13<sup>th</sup>**

### TRACK ONE

**9:00am-10:30am - Session 2a:**

#### Emerging Threats against CI

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

Associate Special Agent in Charge, FBI

#### Drones as a Threat Vector to Critical Infrastructure

- Michael Hill, Program Specialist, Cybersecurity and Infrastructure Security Agency

Doug Cramer, Warning Coordination Meteorologist, National Weather Service

#### Cyber Threats to the US Emergency Services Sector

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

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

#### 11:15am-12:30pm - Session 3a: Communications Sector Symposium



*Communications is key to any community and its infrastructure assets has become increasingly threatened. Without communications, business will be lost, and any emergency coordination would be a disaster. The internet has become a vital part of communications for all. Protection of communication assets and their resilience is vital for*

*businesses, government and all sectors of CI.*

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

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

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

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

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

### TRACK TWO

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

#### Cybersecurity Regulations, Best Practice and Minimum Standards

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

*AI in cybersecurity?*

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

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

Deborah Kobza, President, International Association of Certified ISAOS

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

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

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



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

*of heightened tension.*

Melvin Carraway, Region 4 Security Director, Transport Security Administration

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

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

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

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





## A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

**Wednesday March 13<sup>th</sup>**

### TRACK ONE

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



Communications is key to any community and its infrastructure assets has become increasingly threatened. Without communications, business will be lost, and any emergency coordination would be a disaster. The internet has become a vital part of communications for all. Protection of communication assets and their resilience is vital for businesses, government and all sectors of CI.

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

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

Bob Janusaitis, President, InfraGard San Antonio Members Alliance

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

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

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

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



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

**Securing Your Chemicals: Voluntary Tools and Services to Assess and Mitigate Risk** - Kimberly Heyne, ChemLock Program Manager, Cybersecurity and Infrastructure Security Agency (CISA)

Dan Frazen, CO-CEM, Agriculture Emergency Coordinator (All-Hazards), Colorado Dept of Agriculture  
**Cyber-physical convergence: How cyber incidents can impact the physical world** - Cameron Dicker, Director of Global Business Resilience, FS-ISAC

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

### TRACK TWO

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



The movement of goods and people is vital to a local and national thriving economy. Without a safe, secure and resilient transport network, an economy will crumble. The transport network, from rail, road, air and sea, is at threat from cyber attacks, terrorist threats and natural hazards and its protection and resilience is key for communities and countries to maintain

their economies.

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

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

Head of Sector, Logistics ISAC\*

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

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

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



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

role in CI cyber protection and threat detection?

**The implementation of Zero Trust in Critical Infrastructure** - Ron Martin, Professor of Practice, Capitol Technology University  
Head of Sector, AI-ISAC\*

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

Roman Gonzales, Sr Systems Engineer, Veeam Software, USA



## A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

**Thursday March 14<sup>th</sup>**

### TRACK ONE

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

#### **Modeling and Methodology Around Incident Mitigation & Emergency Management**

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

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

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

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

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

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

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

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

Sarah-Jane Prew, Senior Security Advisor, Arup UK  
Jim Henderson, CEO, Insider Threat Defense Group

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

TBC

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

### TRACK TWO

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

#### **Technologies to Detect and Protect**

*What are some of the latest and future technologies, from ground, underwater, or airspace awareness technologies, access controls, and space based or cyber technology, to predict or detect the wide range of potential physical and cyber threats to CNI. How is AI being utilised in technology to enhance performance.*

**Cyber Resilience** - Senior Representative, Trusted Computing Group

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

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

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

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

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

**11:15am-12:30pm - Session 7b:**

#### **Strategic Resilience Planning**

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

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

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

**Storm-DEPART (Damage Estimate Prediction and Restoration Tool)** - Ollie Gagnon, Idaho National Laboratory

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

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



*A Homeland Security Event For Securing Critical Infrastructure and Safer Cities*

**Thursday March 14<sup>th</sup>**

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

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

*Moderator: John Donlon QPM FSI*

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

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

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

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

Director, Homeland Security and Justice, GAO\*

Senior Representative, FEMA\*

---

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

---

## **Networking Reception**

**Tuesday March 12th**

**5.30pm - 7:30pm**

**Exhibition Floor**

We invite you to join us at the end of the opening day for the Critical Infrastructure Protection & Resilience North America Networking Reception, which will see the CNI security industry management professionals gather for a more informal reception, in a Covid compliant environment.



With the opportunity to meet colleagues and peers you can build relationships with senior government, agency and industry officials in a relaxed and friendly atmosphere.

The Networking Reception is free to attend and open to industry professionals.

We look forward to welcoming you.





*A Homeland Security Event For Securing Critical Infrastructure and Safer Cities*

## The Venue and Accommodation

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



Featuring an on-site casino and live music venues, the L'Auberge Hotel and Casino in Lake Charles only 15 minutes drive from Lake Charles Airport, and less than 2 hours from Houston International Airport. The boutique-style guest rooms at L'Auberge Lake Charles have a flat-screen TV and an additional TV built into the bathroom mirror. Guests will also enjoy the comfort of a plush robe. Plenty of restaurant options, including a buffet, a steakhouse, a sports bar, grille and wine bar, and a café offer a wide variety of meal options for L'Auberge guests. Even the spacious casino floor can't contain all of the fun, wonder and glamour of L'Auberge

Casino Resort! You'll find plenty of ways to pass the time in peerless style with views of the Mississippi River. A fitness centre is available for relaxation. Self-parking is available to hotel guests at no extra charge. Valet parking is also offered.

For more details on the hotel and online booking visit [www.ciprna-expo.com/accommodation](http://www.ciprna-expo.com/accommodation)

## Booking Your Accommodation

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

Promo Code: **STORCH24A**

Book your hotel accommodation at the **L'Auberge Hotel & Casino** at [www.ciprna-expo.com/hotel-booking](http://www.ciprna-expo.com/hotel-booking)

Delegates/attendees can make reservations in the following way:

- Online: Reservations can be made online at [www.ciprna-expo.com/hotel-booking](http://www.ciprna-expo.com/hotel-booking)

**Click on the link, complete your information and quote Promo Code STORCH24A to get your CIPRNA group booking rate.**

**Special Group Rate ends 18th February**

We look forward to welcoming you to Lake Charles.





## *A Homeland Security Event For Securing Critical Infrastructure and Safer Cities*

### Why participate and be involved?

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

Your participation will gain access to this key target audience:

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

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

[www.ciprna-expo.com](http://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](mailto:rayb@torchmarketing.co.uk)

T: +1 559-319-0330

**Paul Gloc**

ROW

E: [paulg@torchmarketing.co.uk](mailto:paulg@torchmarketing.co.uk)

T: +44 (0) 7786 270 820

**Sam Most**

ROW

E: [samm@torchmarketing.co.uk](mailto:samm@torchmarketing.co.uk)

T: +44 (0) 208 123 7909

### Sponsorship Opportunities

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

Some of the sponsorship package opportunities are highlighted here.

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

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

Please enquire for further details.

### Exhibiting Investment

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

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

**Table Top Exhibit 10'x10' - \$4,950**

Raw space with 1 x table and 2 x chairs, pipe and drape, electrical socket, wi-fi, 1 Exhibitor Delegate pass with full conference access, lunch and coffee breaks included, listing in the official event guide and website.

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

**ASK ABOUT OUR BOOKING BUNDLES FOR EXTRA EXPOSURE**

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





*A Homeland Security Event For Securing Critical Infrastructure and Safer Cities*

## Sponsors and Supporters:

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

Platinum Sponsor:



Supported & Co-Hosted by:



Silver Sponsors:



Bronze Sponsors:



Executive Sponsor:



Networking Reception Sponsor:



Coffee Break Sponsor:



Lanyard Sponsor:



Supporting Organisations:



Flagship Media Partner:



Media Supporters:



Owned & Organised by:





## *Join the Community and help make a difference*

Dear CIP professional

I would like to invite you to join the International Association of Critical Infrastructure Protection Professionals, a body that seeks to encourage the exchange of information and promote collaborative working internationally.

As an Association we aim to deliver discussion and innovation – on many of the serious Infrastructure - Protection - Management and Security Issue challenges - facing both Industry and Governments.

A great website that offers a Members Portal for information sharing, connectivity with like-minded professionals, useful information and discussions forums, with more being developed.

The ever changing and evolving nature of threats, whether natural through climate change or man made through terrorism activities, either physical or cyber, means there is a continual need to review and update policies, practices and technologies to meet these growing and changing demands.

Membership is open to qualifying individuals - see [www.cip-association.org](http://www.cip-association.org) for more details.

Our overall objectives are:

- 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

For further details and to join, visit [www.cip-association.org](http://www.cip-association.org) and help shape the future of this increasingly critical sector of national security.

We look forward to welcoming you.



John Donlon QPM, FSI  
Chairman  
IACIPP



## Protecting critical infrastructure from the next pandemic



By Richard Bruns, an economist specializing in cost-benefit analysis of public policy. He works at the Johns Hopkins Center for Health Security.”

A COVID-level pandemic has an annual probability of 2–3 percent, making it a one in 33-50-year event. Most critical infrastructure operations were minimally disrupted by COVID, but a future pandemic could be worse, killing or disabling many working-age people and causing more social and supply-chain disruption. Deliberately engineered pathogens could be

especially dangerous, and they are becoming more and more of a threat as AI tools become more powerful. There are three main steps that critical infrastructure operators can take to ensure continuity of operations in the next natural or deliberate pandemic.

First, continuity-of-operations plans should prepare for a scenario where 20% of all personnel nationwide

are randomly unavailable. Second, there should be plans to house key personnel on-site, away from the community, at the earliest signs of a major pandemic. Third, operators should keep a stockpile of modern PAPR helmets sufficient to maintain operations in a pandemic.

Most current disaster planning assumes a localized disaster, but in a pandemic, critical personnel

will be affected nationwide, in all operations simultaneously. It may not be possible to bring in people with necessary skills from other locations. Operators should examine scenarios where one in five personnel are incapacitated or unable to reach their site, and see what level of operations can be maintained with the remaining staff.

In the earliest days of a future pandemic, we may not know exactly how it is transmitted, or what precautions are necessary. People will have no immunity, and we will not know which age groups are worst affected. Although coronaviruses are more lethal to the elderly, some strains of influenza are highly lethal to people in prime working age groups. This means that the only way to guarantee operations is to keep key personnel fully isolated on site, away from the community, with strong biosecurity protocols for anyone entering the site. This will be expensive and unpopular, and there may be false alarms, but it is a necessary step to survive a lethal future pandemic.

It will always be necessary for some people to travel outside the site or deliver supplies. When they do, they should be wearing a powered air purifying respirator (PAPR). Modern PAPR helmets are almost as easy to use as putting on a motorcycle helmet, and are designed to be worn for extended periods of time in industrial environments. They provide pathogen protection that is far superior to N-95 or elastomeric masks, while also providing head and eye protection. They do not impede breathing, and have a full faceplate that allows the wearer's mouth to be seen.



All critical infrastructure operators should have a PAPR helmet for personnel who leave the job site, or work in close quarters with other people. To ensure that people are comfortable with them in a real emergency, they should practice using them during the peak of the annual flu season. The current list price for an individual to buy a good PAPR is about \$1500, but a large and sophisticated purchaser could probably obtain them in bulk for less than \$500. Even at the high end of the price range, this is cheaper than a few days of sick leave, and much cheaper than the operational disruption that occurs if key personnel are infected.

The three steps of planning for nationwide disruption, planning for on-site isolation, and stockpiling PAPRs will, in combination with current best practices in resilience and disaster planning, dramatically decrease the chances that critical infrastructure operations fail in a future pandemic or biological attack. Incorporating them into disaster preparation strategies will protect us against a future threat that will happen, sooner or later.



## Enriching Critical Infrastructure Security Resilience with Radar



Looking at how radar can assist with critical infrastructure protection with Echodyne

It's no secret that our nation's critical infrastructure, including facilities such as airports and ports, electric generation and transmission plants, water and wastewater treatment facilities, correctional institutions, and chemical, oil and gas, and nuclear sites, face a variety of adversarial threats. Historically, these facilities only needed to be concerned with tracking potential terrestrial adversaries. However,

as drones are becoming more accessible and more common, threats to these facilities have taken to the skies.

Drones are interrupting airport operations, with the Federal Aviation Administration (FAA) now receiving more than 100 reports per month of uncrewed aircraft system (UAS) sightings. The Department of Homeland Security (DHS) and FBI are also seeing more

incidents of drones attempting to damage electric generation and water/wastewater treatment facilities or posing cybersecurity threats to corporations or large data centers. While conventional critical infrastructure security systems consisting of devices such as cameras, thermal sensors, RF sensors, or human guards, have provided adequate critical infrastructure security in the past,

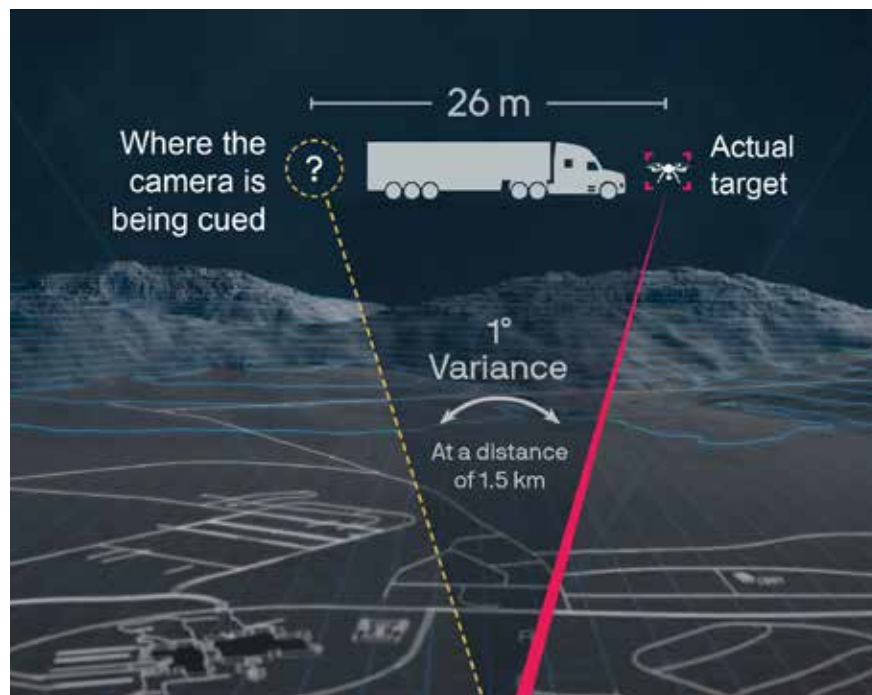
these systems are not sufficient for detecting new aerial threats.

Facilities now need critical infrastructure security solutions that provide enhanced perimeter security coverage both of the air and at greater distances on the ground. This requires a layered solution that includes enhanced commercial off-the-shelf (COTS) three-dimensional radar for simultaneous ground and air surveillance, or focused detection in the highest-risk threat vector. High-performance radar provides the most accurate threat detection data, boosting performance of other sensors in the security stack.

### Why Critical Infrastructure Security Systems Need Radar

Whether curious, clueless, or nefarious, a person, vehicle, or drone can create disruption at critical infrastructure sites by causing harm to people, assets, and operations. And for some sites, a localized disruption can have far-reaching consequences. Imagine the impact to households, traffic flow, health centers, and businesses if an energy transmission site servicing a major metropolitan area goes down due to a threat disturbance.

For critical infrastructure facilities with security solutions deployed at the perimeter, threat visibility may only extend a few feet beyond the fence line and only provides two-dimensional ground-based threat detection. The effectiveness of a short-distance perimeter solution further diminishes at night and in bad weather. Even if an extended or night visibility camera is a part of the system, the optical devices will likely struggle to lock on target and maintain visibility when viewing conditions are not optimal.



### Radar Fills RF Sensor Gaps

Some facilities are enhancing perimeter security by adding aerial monitoring capabilities to their critical infrastructure security systems using radio frequency (RF) sensors – and this is a good step. However, RF sensors have limitations that leave sites with detection gaps:

1. RF alone is unable to detect dark drones, also known as 'silent drones,' since dark drones do not emit an RF signal.
2. Multiple RF sensors are required to achieve threat position accuracy using signal triangulation.
3. RF often displays elevated false-positive rates in urban environments prompted by daily-use devices also emitting RF signals.
4. There are potential concerns over RF "listening" as it pertains to infringing on individual privacy rights.

While RF sensors can lend value as a complementary detector, a comprehensive layered solution for

high-security critical infrastructure requires technology that detects everything that moves on the ground or in the air, even in the absence of an RF control signal. With this in mind, radar is the only detection technology that can provide the required multi-domain detection and tracking coverage. Radar provides precise location and tracking data that can be used independently and in concert with other sensors to improve security outcomes.

### The Benefits of Adding Radar to Critical Infrastructure Security Solutions

For high-risk critical infrastructure sites, the most effective solution for accurate threat detection begins with radar plus pan-tilt-zoom (PTZ) camera integrated with the security team's preferred command and control (C2) and video management system (VMS) software. This combination of technology delivers highly accurate, all-weather, 24/7 detection of air and ground targets, visual confirmation of detected targets, and synced recording of an

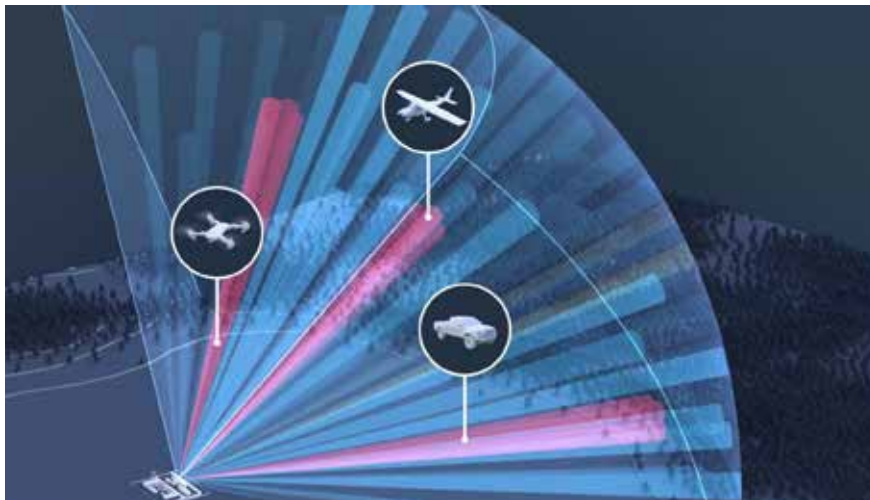


# IMPROVE SECURITY RESILIENCE WITH RADAR

Fill security gaps and improve operational efficiency. Detect and track ground and air threats accurately and simultaneously from a single panel.







object's location data and observed behavior.

The combination of radar detection confirmed by PTZ delivers several operational benefits:

- High-performance radar delivers precise location data and can be used to slew a camera.
- Radar plus PTZ provides more efficient coverage, replacing multiple static cameras along a property line.
- The combination of these two sensors reduces noise and false positives.
- The technology pairing fills a gap that would otherwise require a dedicated team member (e.g. sorting false positives from true targets).

Not only that, if a critical infrastructure team wants to use existing or lower-cost camera equipment, high-performance radar paired with the right video analytics platform will boost operational effectiveness by aiding in dual verification without the need to upgrade existing camera systems. This is a value for security teams who are closing security gaps and assessing risk while developing plans for future-state security system

enhancements.

In addition to providing comprehensive situational awareness, the recorded track data and video can be used to forensically dissect an incident or for prosecuting criminal activity. For sites with higher risk and budgets to support parsing detection technology by type of threat or approach, adding RF detection, below or above ground audio sensors, or other technology may also be appropriate.

#### **Now an Accessible and Valuable Solution for Critical Infrastructure Protection**

Despite the proven value of radar for Defense and national security applications, using conventional phased-array radar systems for critical infrastructure protection (CIP) has never been a practical option. Not only is the cost and size of these historical systems prohibitive, but phased-array radars are designed for much longer-range detection needs and experience challenges with identifying newer drone threats.

But radar technology has rapidly advanced in the last few years. While there are now several small form factor radar options

available that meet basic use case requirements and budget constraints of critical infrastructure sites, most of these options underperform when it comes to providing dependable, comprehensive airspace situational awareness.

A new and innovative design approach called metamaterials has created a breakthrough in radar technology by reducing size, weight, power, and cost (SWaP-C) while retaining accuracy and relative detection distance. The metamaterials electronically scanned array (MESA®) radar is the size of an iPad, weighs less than 5 lbs and packs a power-punch, delivering detection capability symmetrical with drone technology advancements, critical infrastructure use cases, and security budgets.

#### **New Radar Technology is Optimal for CIP**

For critical infrastructure sites seeking to expand their threat detection capabilities, choosing a radar that augments current security solutions and expands situational awareness as threats evolve is paramount. Newly developed high-performance radar is unique and addresses these points by providing three-dimensional coverage, detecting everything moving on the ground and in the air, integrating with existing C2, VMS, and sensors, and delivering military-grade accuracy at a commercially accessible cost – all critical benefits for comprehensive critical infrastructure protection.

When adding radar to a layered security stack, remember not all small form factor radars perform equally. Choosing the right radar for your security risk profile ensures



optimized security coverage, and pain points are addressed including wise use of budget and other resources. For example, a site that has historically placed static cameras at 20-foot intervals along a fence line for defensive coverage can move to a radar + PTZ camera solution for broader coverage with fewer devices. This ability to use technology as a productivity multiplier is particularly important for critical infrastructure security teams that are stretched thin and challenged to do more with less staff and budget.

When researching your radar options, consider this checklist as a guide for identifying features and performance characteristics of radar suited for securing critical infrastructure sites.

#### **Buyers Checklist for Critical Infrastructure Security Radar:**

##### **1. Does the radar deliver equal efficiency, accuracy, and value in both ground and air domains?**

This is especially important for sites concerned with intruder approach from the ground and air. In the age of a changing threat landscape, many critical infrastructure sites

are rethinking their conventional PIDS (perimeter intrusion detection system) solution to include drone detection. A radar that performs equally well in both domains provides a centralized threat detection data source and simplifies systems integration.

##### **2. Will the radar detect threats in multiple domains (drone, human, vehicle, or boat) at the same time?**

Ensuring dual coverage of multiple domains helps future proof the site against emerging technologies and threat tactics.

##### **3. For drone detection, does the radar utilize micro-Doppler to capture a fourth data dimension – velocity?**

The velocity measurement provides users with the speed of a target in a given direction in addition to a target's azimuth, elevation, and range. Processing the micro-Doppler frequency shift is important because it helps radar software distinguish drones from birds, for example. Micro-Doppler also makes it possible to detect hovering drones near or far from a facility and as the drone approaches. This is critical for sites that, in addition to risk of physical breach, have a moderate-to-high-risk of sensitive data being compromised or stolen using a hovering drone carrying a surveillance or data theft device.

##### **4. What is the detection accuracy of the radar? What is the track accuracy?**

As little as a .5% variance in accuracy can result in meters, at distance. Imprecise radar may interpret multiple objects as a single threat and slew cameras to the wrong point in space.

##### **5. Does your radar operate with an open platform and use application**

##### **program interfaces (APIs)?**

Using API integration to request different datasets makes it simple to stream radar data into the fusion layer. There, data from multiple sensors is integrated before being sent to your C2 or VMS software to realize the output of the data, such as slewing a camera.

##### **6. What is the track update rate?**

The track update affects data sharing and integration with other sensors and systems. For example, a 10GHz data exchange rate eliminates the slew lag common in many conventional, small form-factor radar units. The result: cameras slewed using MESA radar data are more likely to retain target lock, seamlessly, throughout an incident.

In summary, radar is a critical sensor for modern security teams seeking to protect, defend, and optimize their efforts in a changing threat landscape. Radar generates precise geolocated tracking data to detect, classify, and track multiple threats at once - accurately and reliably. And certain high-performance radars build on this with the ability to detect all ground and air threats accurately and simultaneously from the same panel.



# critical infrastructure

PROTECTION AND  
RESILIENCE N. AMERICA

March 11<sup>th</sup>-13<sup>th</sup>, 2025

HOUSTON, TEXAS, USA

A Homeland Security Event

## Are you sure your national infrastructure is secure?

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.

## Invitation to Participate

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.

The 7th Critical Infrastructure Protection and Resilience North America will bring together the CI community, leading stakeholders from industry, operators, agencies and governments to debate and collaborate on securing America's critical infrastructure.

As we come out of one of the most challenging times in recent history, off the back of a pandemic, it has stressed how important collaboration in protection of critical infrastructure is for a country's national security.

Join us in Houston, Texas, USA for the premier event for operators and government establishments tasked with managing the region's Critical Infrastructure Protection and Resilience.

For further details visit [www.ciprna-expo.com](http://www.ciprna-expo.com)

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Transportation Systems Sector
- Water and Wastewater Systems Sector

To discuss exhibiting and sponsorship opportunities contact:

Ray Beauchamp  
(Americas)

E: [rayb@torchmarketing.co.uk](mailto:rayb@torchmarketing.co.uk)  
T: +1 408-921-2932

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

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

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

*The premier discussion for securing America's critical infrastructure*

Supporting Organisations:



Help2Protect



Flagship Media Partner:





## Priority Telecommunications Champions: Federal Emergency Management Agency (FEMA) Region 2



### Introduction

The Cybersecurity and Infrastructure Security Agency's (CISA) Priority Telecommunications Services (PTS) mission ensures statewide continuity of communications during an emergency. PTS users have access to three main services that will prioritize your call when networks are congested and degraded. The Federal Emergency Management Agency (FEMA) Region 2 Emergency Communications Team's role is to coordinate within the federal government to make sure

their region (New York, New Jersey, US Virgin Islands [USVI], Puerto Rico and eight Tribal Nations) is equipped to prepare for and respond when disaster strikes. FEMA Region 2 works with a variety of partners to support the whole community effort to achieve the National Preparedness Goal.

About the FEMA Region 2 Disaster Emergency Communications Team

The team consists of Josh Green, David Cucchi, and Joseph Hodge, all FEMA Response Division

Telecommunications Specialists for Region 2, as well as Sabdiel Rivera, External Support Branch Director supporting the Disaster Emergency Communications Team for Region 2. They each bring a unique perspective to the team through their previous work in the U.S. Coast Guard, the Virgin Islands Territorial Emergency Management Agency (VITEMA), and their experience as a telecom lineman and communications specialist. The team's diverse skills and expertise give them the

adeptness to effectively respond to various emergency events and disasters across New Jersey, New York, Puerto Rico, and the US Virgin Islands.

### Putting Priority Telecommunications to Use

The FEMA Region 2 Disaster Emergency Communications (DEC) Team has been championing the use and advocating PTS (Government Emergency Telecommunications Service [GETS], Wireless Priority Service [WPS], and Telecommunications Service Priority [TSP]). When asked why Josh Green and the team use priority services, he responded with conviction, "Bottom line, it is needed." Mr. Green and the team understand the importance of making a connection when you need it most and have more than a few stories to share about the benefits and utility.

On January 6th and 7th, 2020 a magnitude 6.4 earthquake was widely felt throughout Puerto Rico. The FEMA Region 2 DEC Team were flying in to ensure statewide continuity of communications during this emergency when the entire island's power went out. Although small geographically, Puerto Rico is home to over 3 million people. With a large population concentrated in such a small area, the lines of communication become severely congested. Having PTS as part of their emergency response toolkit allowed for the FEMA Region 2 DEC Team to communicate when most needed. Despite telephone line damage due to the earthquake, and massive telecommunication congestion, the team was able to complete 100% (18 out of 18) of GETS calls and 97.89% (371 out of 379) of WPS calls during this disaster.



Since the deadly category 5 hurricane that struck USVI and Puerto Rico in 2017, the number of PTS users in Region 2 has increased. This means more critical emergency personnel are ready and able to respond when a disaster strikes. Despite the increase in users, access to priority communication networks has not degraded; in fact, the number of calls completed using GETS and WPS has increased! In Puerto Rico during Hurricane Maria, September 16, 2017 – October 2, 2017, the completion rate of GETS calls was 88.29% and WPS was 97.35%. Since then, the call completion rate has increased to 100% for both GETS and WPS during Hurricane Ian in the Puerto Rico Region, September 23 – October 2, 2022 both GETS and WPS during Hurricane Ian in the Puerto Rico Region, September 23, 2022 – October 2, 2022.

### FEMA Region 2 Disaster Emergency Communications Team's Practices

#### Preparation is key.

One of Mr. Green's strongest recommendations is for organizations to train employees

on GETS/WPS during their onboarding process. With over 1,000 FEMA Region 2 employees, being prepared is crucial to the success of their mission. To ensure preparation, new employees are given a GETS card and are immediately trained in how to use the services. The Disaster Emergency Communications team have embedded educational training on GETS/WPS within their national safety plans and onboarding processes. Additionally, the team requires all FEMA Region 2 employees, novice, and veterans, to attend a one-hour refresher training on GETS and WPS each year during their "off season".

#### When disaster strikes, it's too late.

Emergency communications requires routine training to ensure successful connections when it matters most. The DEC team in Region 2 have an additional "Just in Time" training. When a natural disaster, such as a hurricane, is approaching, the team comes together for a one-hour emergency communications training to review how to use priority telecommunications services. As Josh Green says, "Don't be the

guy that looks back and made the job harder than it needed to be because of missing a one-hour training!"

**Champions always continue to improve.**

Mr. Green has an eye for continuous improvement! Just like a champion, he sees areas to adjust and is constantly striving to maximize priority telecommunications services. Each month when emergency equipment is tested, Mr. Green would like to incorporate

practice calls using GETS and WPS. This routine exercise may find a connection challenge that can be mitigated before an emergency. Additionally, he would like all employees to download the PTS Dialer App, a user-friendly option that ensures error-free calling at a moment's notice. The app automatically uses the GETS access numbers and the subscriber's PIN. The PTS Dialer App can be set to automatically pull destination numbers from the subscriber's phone contacts or recent calls for

ease of use and seamless priority calling during an emergency. The app is available in the Apple App Store and the Google Play Store.

It is conversations with FEMA team members, like Josh Green, and others who use priority services that help bring home the benefits of these services and encourage other organizations and individuals to enroll.

## TSA Washington breaks record for firearm discoveries in 2023

Transportation Security Administration (TSA) officers in Washington detected 173 firearms in travelers' carry-on luggage in 2022, with the majority of the firearms discovered at Seattle-Tacoma International Airport's (SEA) security checkpoints. Every one of these firearms was discovered during the routine X-ray screening of carry-on property. Nationwide last year, TSA officers found 6,737 firearms at 265 different airports.

The five U.S. airports with the most TSA firearm discoveries are Hartsfield-Jackson Atlanta International Airport, which topped the list with 451 firearm finds. Dallas Fort Worth International Airport came in second with 378 followed by Houston's George Bush Intercontinental Airport with 311; Phoenix Sky Harbor International Airport with 235; and Nashville International Airport with 188. Denver International Airport; Orlando International Airport; Tampa International Airport; Fort Lauderdale-Hollywood International Airport; and Dallas Love Field round

out the Top 10.

In 2023, TSA screened approximately 858 million passengers and crew at airports nationwide. TSA officers across the country discovered firearms in carry-on luggage at a rate of 7.8 firearms per million passengers screened. Stated another way, TSA detected one firearm for every 127,356 travelers screened.

The busiest airport in Washington is SEA where TSA officers screened approximately 19.7 million departing passengers and crew, which ranks 14th busiest for TSA security checkpoint screening operations. Statistics show that TSA discovered one firearm for every 171,221 travelers screened at SEA, which is below the national average.

"TSA in Washington set a record for the number of passengers and crew screened in 2023, but we also set a record for the number of firearms discovered in travelers' carry-on luggage. This is not the type of record we want to set in the Evergreen State," said TSA Acting Federal Security Director

for Washington Chris Hadinger.

"I am hopeful that anyone who is planning to travel with a firearm on a commercial aircraft in the New Year will review the procedures for doing so properly to avoid becoming a statistic."

When a TSA officer sees the image of a firearm on the X-ray screen, TSA immediately notifies the local airport law enforcement agency, which responds to the security checkpoint. A law enforcement officer removes the firearm from the X-ray tunnel and makes contact with the traveler. What happens to the firearm and the traveler is up to the discretion of the airport law enforcement agency.

In addition to potential criminal citations for bringing a firearm in carry-on luggage, TSA can levy a civil penalty against the traveler. Among the factors TSA considers when determining the civil penalty amount include whether the firearm was loaded and whether there was accessible ammunition. Even if a traveler has a concealed weapons permit, firearms are not permitted in carry-on luggage.



## Stress testing Chile's critical infrastructure resilience with a multi-sectoral approach

In a trailblazing event held recently, a workshop focusing on infrastructure resilience was conducted in Santiago, organized by the Technical Working Group on Infrastructure Resilience. This initiative was convened by the National Service for Disaster Prevention and Response (SENAPRED) to delve into the knowledge and contributions that public entities and infrastructure operators can make to strengthen the resilience of infrastructure systems.

This activity is part of the international project "Enhancing Infrastructure Resilience through Strengthened Governance," supported by the Coalition for Disaster Resilient Infrastructure (CDRI) and the United Nations Office for Disaster Risk Reduction (UNDRR). The project aims to increase knowledge and understanding of vulnerability and resilience among infrastructure stakeholders, develop the national capacity to consider risk in infrastructure planning and implementation, and foster collaboration and knowledge exchange among relevant actors for this purpose.

The workshop, convened by SENAPRED, involved the participation of various government ministries, including the Ministries of Energy, Health, Education, Public Works, Transportation and Telecommunications, Defense, Social Development and Family, and Housing and Urban Development. In addition, there were also representatives from CDRI and UNDRR, the United Nations Resident Coordinator's Office (RCO) in Chile,



the United Nations Operational Satellite Centre (UNOSAT), and the International Coalition for Sustainable Infrastructure (ICSI). These institutions are active in the project's implementation and technical development in the country.

Over two days, attendees engaged in rigorous efforts to stress test the country's critical infrastructure networks and evaluate the state of infrastructure practices using the Principles for Resilience Infrastructure scorecard, which is an integral component of the global methodology developed by CDRI and UNDRR.

The workshop aims at identifying the main threats and vulnerabilities of Chile's infrastructure and estimate the combined risk they pose to the country and its economic sectors. The collaboration and exchange of perspectives among participants were particularly beneficial, resulting in a thorough and multidisciplinary analysis.

The main findings include the need for tailored mitigation and preparedness strategies, the

importance of strengthening critical areas to ensure resilience and response in emergency situations, and the relevance of cross-sectoral collaboration for more effective risk management.

One of the participants, Carlos Salinas from the Ministry of Energy, noted, "(...) These types of activities are relevant not only to contribute and learn from knowledge but also to connect with colleagues from other sectors working on the same issues, allowing us to establish or strengthen cooperation to address risks." Similarly, Colonel Cristian Aparicio from the Ministry of Defense highlighted that "(...) in these activities, in addition to making our small contribution, it reinforces our commitment to the country's needs and shortcomings towards a comprehensive view of risk reduction, particularly in a complex issue such as critical infrastructure."

This workshop marks a milestone in Chile's efforts to move towards more resilient infrastructure, prepared to face current and future challenges. Over the next few months, the results of this workshop are expected to be consolidated, and an implementation plan will be defined to advance the establishment of more resilient infrastructure in Chile. These plans will be discussed and validated through another workshop to be held sometime in early 2024. Throughout these activities, Chile is making progress in building the necessary capacity and preparedness to reduce disaster risks and anticipate future challenges, particularly in the context of climate change.

## An Interview with CISA



Ben Lane, CIPRNA event manager, caught up with Terence Check, Senior Counsel – Infrastructure Security, at the Cybersecurity and Infrastructure Security Agency (CISA).

**Ben Lane (BL):** Can you tell us, broadly, about your career to date and why you choose this career.

**Terence Check (TC):** Growing up in the Midwest in a diasporic community of Hungarian immigrants who had fled war, violence, and political oppression, I was acutely aware of history, geography, and civics issues at a young age. This grew into a keen interest in international affairs, national security, which naturally led me to a career with the federal government. After obtaining my J.D. and an LL.M in National Security Law and



Terence Check, Senior Counsel – Infrastructure Security, Cybersecurity and Infrastructure Security Agency (CISA)

Policy, I have worked with the U.S. Department of Homeland Security since 2015. DHS has a fascinating, broad, and varied mission that touches everything from counterterrorism to cybersecurity to emergency management. Every day has the possibility of working on a new or different national security problem.

**BL:** Can you outline your present role as Senior Counsel for Infrastructure Security in the U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) Office of



Chief Counsel and your position as “advisor on constitutional and national security law issues in support to CISA’s critical infrastructure security mission”.

**TC:** At its core, my practice involves the study of the Constitution, an enduring framework for organizing our government in times of fair weather or foul (quite literally). Mainly, I advise CISA’s Executive Assistant Director for Infrastructure Security, his Deputy, and his senior staff on legal issues that arise in the course of their daily operations with an emphasis on the statutory contours of their legal authorities. This makes my practice as wide as CISA’s mission, so on a given day, I might analyze legal issues spanning from school safety to cyber information sharing to disaster planning and response.

**BL:** In your abstract and a topic for your presentation at CIPRNA 2024 you say: “see something, say something” but many owners and operators of critical infrastructure might hesitate to share information

with the federal government. Can you expand on what you mean and provide a short case study?

**TC:** In the United States, the overwhelming majority of our critical infrastructure is owned by private or non-federal entities. As I said before, national security law is mainly the study of our Constitution, and our Constitutional framework makes federal authority one of limited scope. But many owners and operators interact with federal regulatory agencies, and many understandably struggle with sharing threat information when doing so might lead to legal or economic consequences. Consider a scenario where a manufacturer of heavy machinery discovers a vulnerability in their custom software: warning their customers and the government might help prevent a major security incident. But sharing this information might expose proprietary details or create some reputational risks. Luckily, CISA oversees a couple of legal regimes that help to reconcile these

at-times competing considerations. These regimes include PCII and CISA 2015, you can read more about them at <https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing>.

**BL:** How do you see legislation changing that might include operators to be ‘forced’ to share information, or meet minimum standards of security?

**TC:** To this point, the United States has employed a largely voluntarily approach to sharing cyber and other types of threat information. Though there are several new regulatory developments in the field of cybersecurity (for example, the enactment of the Cyber Incident Reporting for Critical Infrastructure Act), I myself feel that legislative development should come alongside a growth in corporate responsibility in cybersecurity. Director Easterly has spoken about this at length, and I share her views that we largely need a cultural change: where cybersecurity is considered a niche IT issue, and to get to the point where ensuring good cybersecurity and data management practices becomes a core business issue.

**BL:** Briefly explain the work of your department in reducing risk and its importance to overall CI strategies.

**TC:** CISA truly has a wide range of service and informational offerings that can assist stakeholders as large as Fortune 500 companies or as local as your neighborhood elementary school—and everywhere in between. Our recent efforts have focused on assisting sectors that are highly attractive targets to cyber bad actors but lack many of the resources, capabilities or investments needed to achieve the necessary level of cybersecurity.



Healthcare, water systems, and educational institutions have become a particular area of focus. As the national coordinator for infrastructure security, CISA works closely with “sector risk management agencies”, which are parts of the federal government that have particular expertise and capability to help reduce risk to a particular sector or sub-sector of our economy.

BL: What keeps you awake at night?

TC: We have a good understanding of known national security risks

like terrorism and cyber-attacks. These kinds of risks have led to the creation of CISA and the Department of Homeland Security. I worry about mid or far future risks or risks that have no kind of predictability. I would like to see new legal and policy work that gives DHS the authority to address these kinds of challenges.

BL: Thank you and looking forward to seeing you in Lake Charles this March.

TC: Thank you Ben, also looking forward to it.



## NSA Releases Recommendations to Mitigate Software Supply Chain Risks

In response to an increase in cyberattacks to supply chains over the past five years, including targeted attacks of software supply chains, the National Security Agency (NSA) is releasing the Cybersecurity Information Sheet (CSI), “Recommendations for Software Bill of Materials (SBOM) Management.”

This CSI provides network owners and operators with guidance for incorporating SBOM use to help protect the cybersecurity supply chain, with a focus on and some additional guidance for National Security Systems (NSS).

Effective Software Bill of Materials (SBOM) management leverages identification of software components to mitigate cyber risk and support improved cybersecurity throughout the software’s lifecycle. According to the CSI, SBOM management should proceed in three steps. First,



examine and manage risk before acquiring software. Second, analyze vulnerabilities after deploying new software. Third, implement incident management to detect and respond to new software vulnerabilities during vital operations.

“As Software Bills of Materials become more integral to Cybersecurity Supply Chain Risk Management standards, best practices will become critical to ensuring efficiency and reliability of the software supply chain,” said Rob Joyce, NSA Cybersecurity Director and Deputy National Manager for the

National Security System (NSS). “Network owners and operators we work with count on NSA to advise them on shoring up their defenses. These guidelines provide the information they need to select the appropriate tools to reduce an organization’s overall risk exposure.”

This guidance includes recommended SBOM tool management functionality that supports the Director of the NSA in his role as the National Manager for National Security Systems, namely to provide better Cybersecurity Supply Chain Risk Management (C-SCRM) for NSS owners and operators. The CSI encourages NSS owners to implement a robust C-SCRM SBOM management strategy that ensures the authenticity, integrity, and trustworthiness of software products.

## An Interview with FS-ISAC



Ben Lane, CIPRNA event manager, met with Cameron Dicker, Director of Global Business Resilience at the Financial Services Information Sharing and Analysis Center (FS-ISAC). FS-ISAC is the member-driven, not-for-profit organization that advances cybersecurity and resilience in the global financial system, protecting the financial institutions and the people they serve.

Founded in 1999, the organization's real-time information sharing network amplifies the intelligence, knowledge, and practices of its members for the financial sector's collective security and defenses. Member financial firms represent \$100 trillion in assets in seventy-five countries.

**Ben Lane (BL):** Hello Cameron. Good to meet. Can you provide a little bit about yourself, a plotted history of your career and your position now?



**Camron Dicker, Director of Global Business Resilience, FS-ISAC**

**Cameron Dicker (CD):** I joined FS-ISAC in June of 2022, where I serve as the Director of Global Business Resilience. I focus on running resilience programs across our various regions, including the Americas, Europe, Middle East and Africa, and Asia Pacific.

In these regions, my team runs a business resilience committee. This is a committee for our membership that brings members together to discuss best practices and identify risks. During an incident we assess

the operational risks and systemic nature of a disruptive event. And of course, write, manage, and update playbooks.

In addition to the business resilience committees, my team also runs our exercise program. Once we have the playbooks, we evaluate those playbooks. We run exercises on all hazards, from hurricanes to insider threats to cyber. Anything that could pose a disruption to the sector's ability to operate. We evaluate the sector-level playbooks to identify any gaps in policy, process, and procedure. We also build muscle memory while working with organizations, as well as with our government partners, during a disruptive event. So, when those bad days happen, we know who is going to do what, when, and how.

Before joining FS-ISAC, I worked for the Department of the Treasury, where I was the Deputy Director for Response and Recovery within the Office of Cybersecurity and Critical Infrastructure Protection. Prior to that I was at the Federal Reserve.

**BL:** Thank you for the introduction. Can you provide an explanation of FS-ISAC and its roles and objectives?

**CD:** FS-ISAC is a member-driven organization designed to collect, analyze, and share information that better prepares organizations to be more resilient to any hazard or disruption. We do this through three pillars, intelligence, security, and resilience, which is my department.

Our global intelligence office collaborates with members to share information in an anonymized, trusted environment when they have an incident or any sort of event. We then analyze that information, add in other information we receive



from vendors, other members, government sources, and then put that back out to the membership through our channels to help them better understand threats and how to mitigate them.

Through our security pillar, we share all kinds of information and insights related to the work of protecting the firm. We do this through a wide variety of member-only conferences and events, as well as through our communities, which are smaller groups within our 5000-firm membership that relate to common interests, be they regional, sub-sector, topic or even role.

And then our resilience work is focused on developing incident response playbooks and then continuously testing and improving those through exercises. Of course, the pillars are inter-related and feed each other to continuously achieve our mission of advancing cyber security and resilience of the global financial system.

**BL:** It is a virtuous circle. Let us delve a bit deeper into these topics. What

are the main developments and changing threats you are seeing now for the financial services sector?

**CD:** I think the reliance on third parties and the emergence of third-party suppliers as a primary attack vector for the sector is the largest change we have seen over the last few years. Threat actors have learned if they attack one bank, they will get one score but if they attack a third party who serves multiple firms, they will potentially get hundreds, if not thousands. Many third parties are not regulated in the same way banks are, and do not have the same security programs that a large, well-resourced financial institution will have. In some cases, they may be the easier way into the bank than the bank itself.

So, from a threat actor's perspective, it makes total sense to focus on providers.

**BL:** Interesting. I am sure this topic will be discussed in more detail at CIPRNA this year. How does FS-ISAC work within its industry sector to tackle and prepare its members





for these changing threats? We have talked about information sharing, but can you dive a little deeper into this area?

**CD:** FS-ISAC is a wide collection of nodes around the world – our 5000-member firms who essentially act as a real-time sensor network for the cyber threats facing the sector. We see attacks happen every day. Our members report things that worked, things that were unsuccessful, and how they fought against it. We can then start to pick up trends, the emerging threats, and where they are moving from market to market.

We also work closely with our public sector partners in several jurisdictions to take the information the government is seeing, combine it with the information we are seeing, and then provide insight back to our members. It then goes into these communities, where they can brainstorm and talk about what has worked at some organizations and not worked at others, to share best practices for how the organizations can defend against the threat landscape.

And then, where my team really comes in, is our exercising function.

As we see threats start to emerge, we can exercise with the members against these. We can figure out what we think is going to happen, what the potential disruptive effects are, and what we can do today to prepare for the threats of the future.

In 2023, for example, we had a couple exercises working on the emerging threat of AI, as well as risks associated with the potential use of post-quantum computing to break cryptography used by the sector. This allows us to think through what those threats could be in two, three, four years' time, and start now with recommendations that financial firms can use.

**BL:** It is fascinating that you look three to four years ahead. That is predicting a long way ahead in such a fast-moving world. We have talked about FS-ISAC as an individual body. How does FS-ISAC work with other sectors and other ISACs to ensure resilience in the system?

**CD:** In the United States there is the Council of ISACs. It has representation from all the critical infrastructure sector ISACs, of which we are a member. We participate very, very actively in that forum to make sure we have contacts with all

the other ISACs, that we are sharing information on a regular basis, and we are coordinating on that front.

FS-ISAC is heavily dependent on energy and telecommunications. So, we have a tri-sector, which is just those three ISACs in a close, trusted community, sharing information on a regular basis about the threats and risks we see. We also have a playbook specific to how these three ISACs would coordinate in a state of heightened awareness or an actual incident because of the strong interdependencies between these three sectors.

**BL:** You are dealing with a lot of information. Incredible work. What are the main challenges for critical infrastructures, do you foresee?

**CD:** My personal view on this and having watched this grow during the past few years, is that the greatest risk we are going to see over the next few years is the interconnectedness between organizations and between sectors. We do not live in a world anymore where it is sufficient to say, "I know what I own, and I can protect it." It is about who you are connected to. Who you rely on. And what permissions they have into your network, or what relationships they have with you that could disrupt your ability to function.

The high reliance on IT is part of that, but it is not everything. There is still a reliance, as a bank for example, on their ability to receive physical currency, which is a reliance on the Federal Reserve, and a reliance on the Mint to print it, and a reliance on the armored carriers to deliver it. There is a lot in the chain to make these things happen. We are no longer in an environment where one piece is going to operate effectively without the others.

**BL:** That is a great answer. And again, a topic which will be discussed in further detail at CIPRNA this year. Cameron, thank you for your time. We look forward to seeing you in Lake Charles March 12 to 14 where you'll be speaking in the Critical Industries Sector Symposium: <https://ciprna-expo.com/session/critical-industries-sector-symposium/>.

Thank you.

**CD:** I am really looking forward to it. Thank you.

#### **About Cameron Dicker, Director of Global Business Resilience, FS-ISAC**

*Cameron Dicker is the Director of Global Business Resilience at FS-ISAC and the Deputy Director of the Financial Services Sector Coordinating Council. As Director of Global Business Resilience, Cameron oversees FS-ISAC's exercise programs as well as the regional business resilience committee. Prior to joining FS-ISAC, Cameron worked on resilience*

*policy and crisis management for the Department of the Treasury and the Federal Reserve Board. Cameron earned his master's degree in philosophy from San Francisco State University and his bachelor's degree from Drake University. He is based in the Washington DC-Baltimore area.*

## **CISA and FBI issue guidance on Chinese-manufactured UAS for critical infrastructure owners and operators**

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) issued a warning to increase awareness of potential threats associated with Chinese-manufactured Unmanned Aircraft Systems (UAS). They also provided recommendations for cybersecurity measures to help protect networks and sensitive data for critical infrastructure entities, as well as state, local, tribal, and territorial (SLTT) partners.

Titled 'Cybersecurity Guidance: Chinese-Manufactured UAS,' the cybersecurity guidance identified that the People's Republic of China (PRC) has enacted laws that provide the government with expanded legal grounds for accessing and controlling data held by firms in China. The use of Chinese-manufactured UAS in critical infrastructure operations risks



exposing sensitive information to PRC authorities.

Additionally, the guidance outlines the potential vulnerabilities to networks and sensitive information when operated without the proper cybersecurity protocols and the potential consequences that could result. The guidance also provides additional resources to augment an organization's preparedness, response, and resilience.

The PRC's collection of sensitive information and potential network

access obtained from Chinese-manufactured UAS may result in significant consequences to critical infrastructure security and resilience. Acquisition of such data or network access has the potential to advance the PRC's strategic objectives and negatively affect U.S. economic and national security by exposing intellectual property to Chinese companies and

jeopardizing an organization's competitive advantage.

It also included providing enhanced details of critical infrastructure operations and vulnerabilities increasing the PRC's capability to disrupt critical services; compromising cybersecurity and physical security controls leading to potential physical effects such as theft or sabotage of critical assets, and exposing network access details that enhance the PRC's capability to conduct cyber-attacks on critical infrastructure.

# The Imperative for Resilience-based Critical Infrastructure and National Preparedness

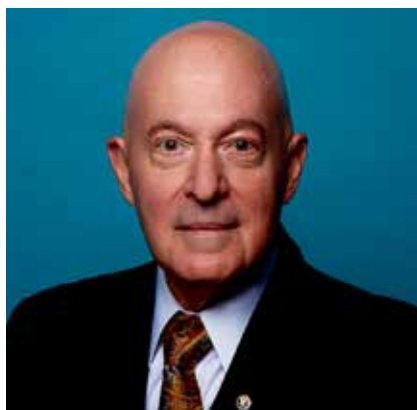


Jeff Gaynor is the President of American Resilience, LLC. He brings six decades of Critical infrastructure (CI) experience and innovation to correcting America's preparedness trajectory.

*"Status quo you know is Latin for the mess we are in."*

*President Ronald Reagan*

It has been 18 years since the Homeland Security Advisory Council (HSAC) recommended: "... Critical Infrastructure (CI) Resilience as the top-level-strategic objective - the desired outcome to drive national policy and planning." Further, it has been 13 years since the HSAC's Community Resilience Task Force recommended the conduct of an "American Resilience



Jeff Gaynor, President of American Resilience, LLC.

Assessment" and nine years since Presidential Policy Directive 21 made "Critical Infrastructure Security and Resilience" America's CI preparedness goals.

Consistent with President Reagan's observation, while the term resilience is commonplace in popular lexicon and feels good, evidence of resilience-based CI and National Preparedness remains increasingly conspicuous in its absence. America has effectively homogenized the term



resilience into iterations of the objectively unmeasurable and clearly inadequate 1990's era CI and National Preparedness status quo. As a result, America's Preparedness trajectory is, by the millisecond, making the nation the most exploitable, exploited, consequence enabling and multiplying in its history. Making matters worse, precisely at the time America needs increasing levels of energy to make itself "green," it has restricted domestic energy production, sold its oil reserves and allowed itself to become increasingly reliant on a nation that is decisively engaged in transforming America's CI into vectors to inflict, if not unrecoverable, unprecedented consequences upon our nation.

***We can't solve today's problems with the mentality that created them."***

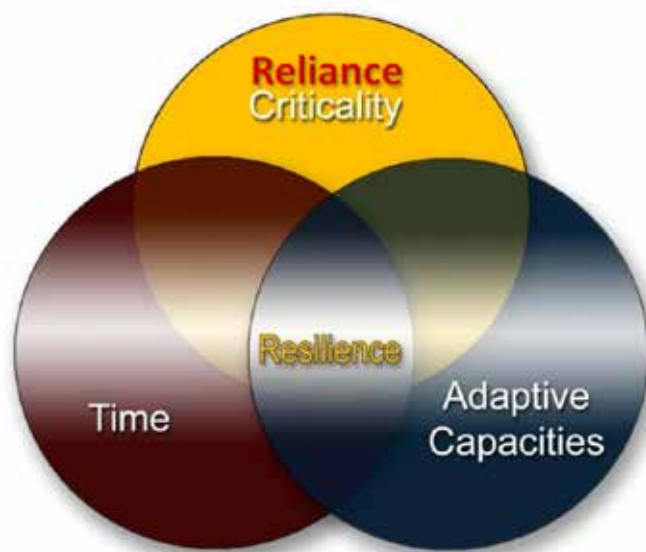
*Alfred Einstein*

Consistent with the above, the long-standing question remains: What must America do to correct its CI and National Preparedness status quo and "... the mess we are in?"

First: Rhetoric is not Results:

America must finally implement an operationally proven, objectively measurable, nationally comprehensive and compatible preparedness goal, culture and condition. Specifically, a culture and condition that provides for: The predictable provision of CI products and services© and (short of Global Armageddon), the continuity of the spectrum of American Life.

To those ends and at a minimum: Implement Resilience-based CI protection, cybersecurity and National Preparedness mindsets, metrics, methodologies and technologies.



© Copyright American Resilience, LLC 2011 – 2024 – All Rights Reserved

#### Resilience-based Mindsets

While anything but a comprehensive list:

- Add Reliance to your risk elements and assessments.
  - Never be reliant on anything you can't quantifiably protect, secure or control.
- Accept no CI single point of failure (e.g., automated systems).
- Respect "The Predator's View" (i.e., the view from outside looking in).
- Remember Sun Tsu: "The opportunity of defeating an enemy is provided by the enemy himself"
  - Everything is a target.
  - Public pronouncements, behaviors and advertising raise predator awareness and target values.
- Objectively unmeasurable goals are unachievable.
- Equalize Resilience-based CI protection, cybersecurity and national preparedness efforts across the event continuum (Prevention and Continuity, Response and Recovery).

- "Lessons Learned" not acted upon are consequence enablers.
- The only acceptable "New Normal" is one superior to its predecessor.

#### The Resilience Metric

Time is a universally accepted metric and the metric of resilience. It makes resilience-based CI and National Preparedness objectively measurable across the spectrum of American Life.

Resilience-based Preparedness Methodology

***"If you can't explain it simply enough you don't know it well enough"***

*Alfred Einstein*

Consistent with Einstein's quote, illustrated below is the practice and culture of resilience.

Resilience is simply the convergence of continuously knowing:

- What you are reliant upon and thus critical to you.
- How long you can be without what is critical to you and,
- having proven adaptive

capacities/failovers to ensure you can have what is critical to you within the time you are willing to be without it.

Thus, resilience is a nationally comprehensive and compatible, equitable, objectively measurable, operationally proven and cost neutral CI and National Preparedness process, culture and resulting condition. Uniquely, resilience allows people, businesses, and communities throughout the nation to work first in their best interests to the best interests of all.

#### Resilience-based Technologies

- Make America's CI SMART+ Resilient (Smarter).
  - o Implement historically proven, "Back to the Future" solutions.

- Mandate physical overrides and people trained and annually certified to operate them for all high consequence producing networked/automated systems.
- Keep hard copies of all vital/ consequence producing information.

#### The Bottom Line

*"States are like people. They do not question the awful status quo until some dramatic event overturns the conventional and lax way of thinking."*

*Dr. Victor Davis Hansen Military Historian & Hoover Institution Senior Fellow*

America must stop learning the hard way! To ensure its safety, security, quality of life and future,

America must accept the growing presence of domestic and global threats and to prevent the otherwise guaranteed infliction of consequences of unprecedented scope, duration and intensity, build resilient infrastructures that can, in the words of a 1950's era Timex Watch Commercial: "Take a lickin' and keep on tickin'."

## U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure

A December 2023 court-authorized operation has disrupted a botnet of hundreds of U.S.-based small office/home office (SOHO) routers hijacked by People's Republic of China (PRC) state-sponsored hackers.

The hackers, known to the private sector as "Volt Typhoon," used privately-owned SOHO routers infected with the "KV Botnet" malware to conceal the PRC origin of further hacking activities directed against U.S. and other foreign victims. These further hacking activities included a campaign targeting critical infrastructure organizations in the United States and elsewhere that was the subject of a May 2023 FBI, National Security Agency, Cybersecurity and Infrastructure Security Agency (CISA), and foreign partner advisory

. The same activity has been the subject of private sector partner advisories in May and December 2023, as well as an additional secure by design alert released by CISA.

The vast majority of routers that comprised the KV Botnet were Cisco and NetGear routers that were vulnerable because they had reached "end of life" status; that is, they were no longer supported through their manufacturer's security patches or other software updates. The court-authorized operation deleted the KV Botnet malware from the routers and took additional steps to sever their connection to the botnet, such as blocking communications with other devices used to control the botnet.

"The Justice Department has disrupted a PRC-backed hacking

group that attempted to target America's critical infrastructure utilizing a botnet," said Attorney General Merrick B. Garland. "The United States will continue to dismantle malicious cyber operations – including those sponsored by foreign governments – that undermine the security of the American people."

"In wiping out the KV Botnet from hundreds of routers nationwide, the Department of Justice is using all its tools to disrupt national security threats – in real time," said Deputy Attorney General Lisa O. Monaco. "Today's announcement also highlights our critical partnership with the private sector – victim reporting is key to fighting cybercrime, from home offices to our most critical infrastructure."

## Energy Infrastructure Bandages or Long-Term Resiliency – Time to Get Serious



Scott Sklar is an Adjunct Professor at The George Washington University teaching three unique interdisciplinary sustainable energy courses and is the Sustainable Energy Director at GWU's Environment and Energy Management Institute (EEMI).

In the last thirty years, the industrialized world has transformed two networks to self-healing grids. Communications moved from copper, to fiber-optics, satellites and cell towers in what has become a self-healing grid. Cell towers and communication satellites fail with regularity and the working cell towers or satellites in nanoseconds triangulate around the failed infrastructure and the communications system continues working without a blip.

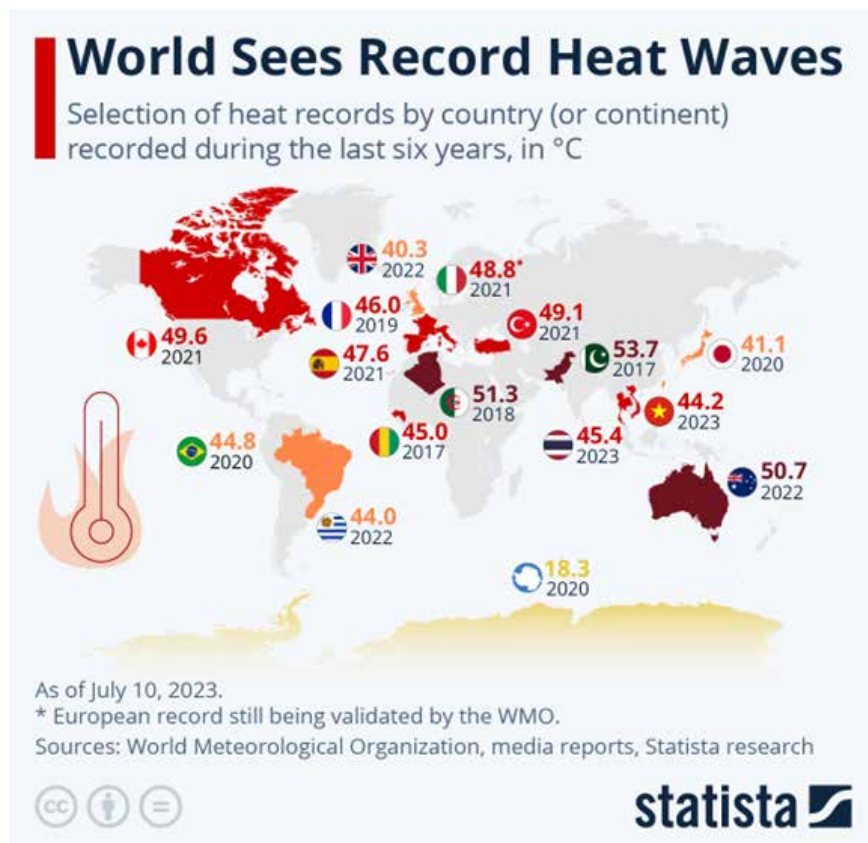


Scott Sklar, Adjunct Professor, The George Washington University

The Internet, while it relies on the communication networks, - its brains, data centers, also have the capability to compensate for failure of one data center where other data centers, take over accessing "the cloud" so that one failure does not impede overall access to data.

But our electric grids have three competing approaches in a rather stumbling way – band aids on the existing grid, smart grids, and





microgrids-distributed generation tied to energy storage.

For the electric grid, whether it's the electric provider, the utility, -- or the user -- industrial, commercial infrastructure, government, residential -- most instances the existing system is propped up or backed up. Transmission and distribution lines are restrung, spinning reserves added, and end users using back-up generators, battery banks. Unfortunately, as billion-dollar plus disasters have quadrupled in the US, and super-heat waves have sextupled globally, the old way is not going to withstand the extreme wind gales, super-heat & super-cold waves, cyber attacks & terrorism, vandalism, human error, and damage from animals.

Propping up the traditional electric grid, in a business-as-usual approach is destined to fail. And in most of the world -- developing

countries to the industrialized world are all experiencing more outages and longer outages. The response is woefully inadequate.

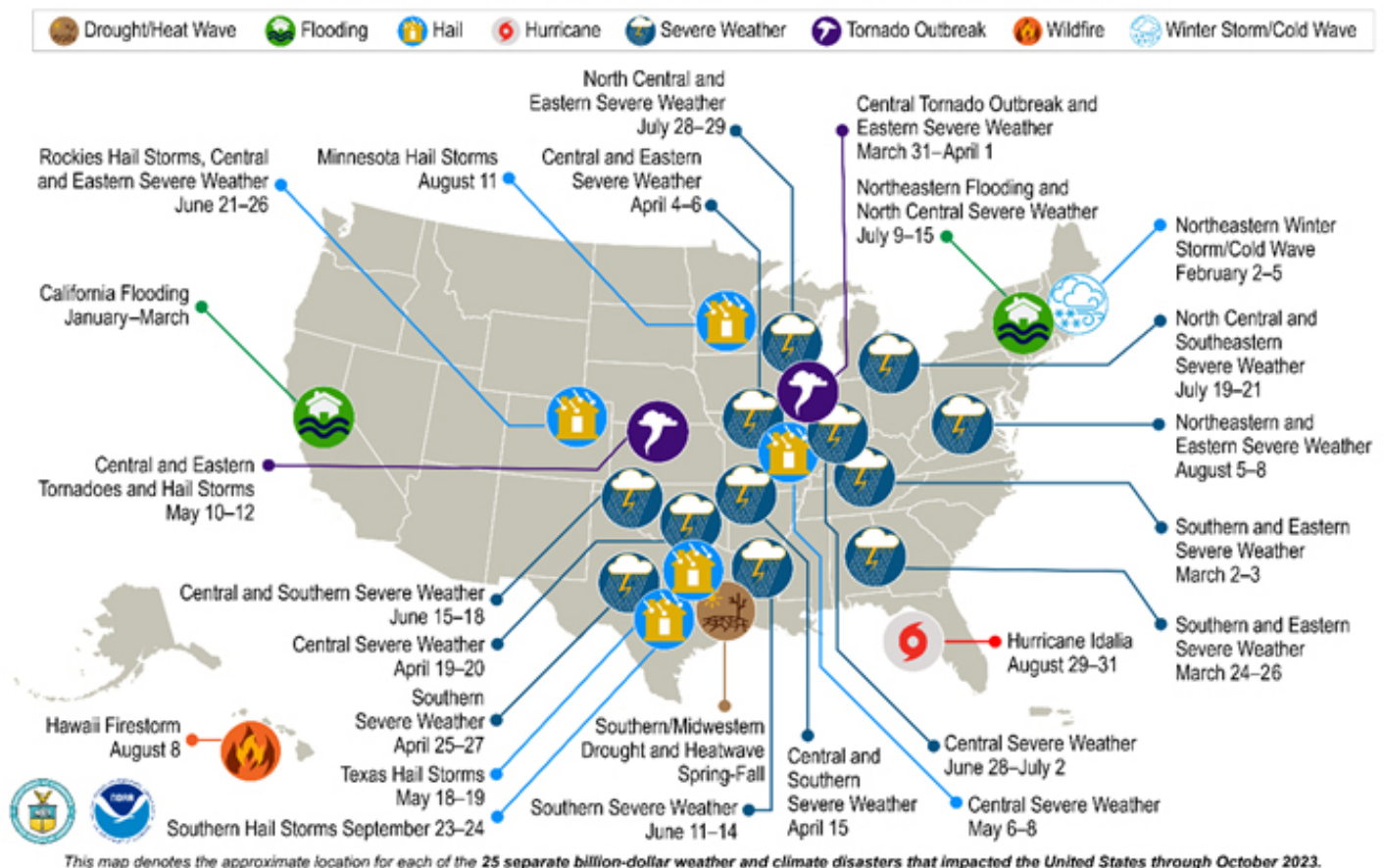
Frankly, the two divergent approaches that are set to leapfrog electricity resiliency and reliability are also inadequate.

The first approach is to make the electric grid "smarter", adding sensors and controls -- since most electric utilities don't even know there is an electric power outage until a customer actually calls them. Use of smart meters, incorporating all types of energy storage such as pumped hydropower, batteries, flywheels, compressed air & liquids, gravity systems, thermal storage, and even hydrogen, are important steps. Use of higher-flow electric wires and implementing energy efficiency programs to reduce electricity draw by customers are also critical. Innovative programs to increase use of building

insulation, establish energy labels for appliances and office machines --- energy efficiency is always less expensive and faster than any kind of electric energy generation. But this streamlining the existing electric grid will not in-and-of-itself result in the electricity reliability and resiliency electricity consumers need as these external threats increase exponentially.

The second approach focuses also on energy efficiency, but also distributed electric generation along powerlines and substations, at points of end use. Within that scenario "smart buildings" or "green buildings" are also a key approach which incorporate high-value energy efficiency on the building envelope as well as the heating & cooling system, and appliances which reduces electric load, and then on-site energy generation for both heating & cooling and electricity. Solar water heating geothermal heat pumps, small wind systems, wood stoves, biogas units are multibillion dollar industries globally. And for electricity - solar photovoltaics, small wind energy, microhydropower, fuel cells tied to smart battery banks have grown exponentially.

Within this approach is evolution of microgrids which blends on-site multiple technologies including traditional small generators, blends of renewable electricity generation along with energy storage, mostly smart battery banks. These microgrids have capability to seamlessly separate from the electric grid to power buildings, campuses, infrastructure. And when the electric grid stabilizes, the microgrid can seamlessly reconnect to support and/or interact with the



electric grid. A huge percentage of microgrids also provide electricity for off-grid electric loads mostly for critical infrastructure such as cell towers, pipeline pumps for fuels-water-sewage, hospitals, first responders (police, fire, ambulance), gas station pump islands and EV charging, airport runways, seaport communications, water & sewage treatment plants, and many other essential uses.

All this is nice, but the haphazard and divergent pathways have actually made us feel better, and in some cases have added some reliability but have not yet met the overall resiliency, reliability, or emissions goals their supporters have claimed.

Policymakers and regulators need to step up and drive a convergence

while accelerating the changeover. This means reliance of pure central station electric generation while propping up power lines won't do the job. The situation requires amping up grid modernization whole hog – meaning rapidly enhance the smartness, the and all sizes of electric power from transmission-to distribution to end use. At the same time, push the user side -- so buildings, infrastructure, and campuses – corporate, government, institutions aggressively save but also generate most, if not all their electric power.

Frankly it requires a massive push from both ends of the energy system – supply & delivery as well as energy end use autonomy. Waiting around, or going slow will result in higher energy costs, shadow

resiliency, and increasing loss of reliability leaving millions of users in the dark. We all know better.

# CISA 2023 - A Year in Review Showcasing Efforts to Protect Critical Infrastructure

2023 Year in Review Details CISA's Work to Manage Cyber and Physical Risk in Communities Across the Country



The Cybersecurity and Infrastructure Security Agency (CISA) released its fourth annual Year in Review showcasing CISA's work to protect the nation from cyber and physical threats, while working to increase the resilience of critical infrastructure Americans rely on every day. The 2023 Year in Review reflects on the agency's accomplishments across its broad cybersecurity, infrastructure security and emergency communications missions as the nation and the world adapted to technological advances, spillover from international events and other major events. In 2024, CISA will continue to develop and deliver tools, training, technical expertise and other resources to help our critical infrastructure partners increase their own resilience and defenses against evolving risks.

"This Year in Review report demonstrates CISA's exceptional work in 2023 to protect critical infrastructure," said CISA Director

Jen Easterly. "It not only celebrates our progress from the past year but also spotlights groundbreaking milestones and pioneering 'firsts' achieved by the agency. These efforts are a testament to and reflect the dedication of CISA's workforce. Because of their commitment to the mission, the critical infrastructure systems that Americans rely on every day are more secure and resilient than ever."

In 2023, the CISA accomplishments included:

- Promoting Secure by



Design Principles. As part of an Administration-wide push to promote secure software development, CISA launched its Secure by Design campaign in April 2023. This effort strives for a future where technology is safe, secure and resilient by design by encouraging software manufacturers to take ownership of customer security outcomes. In October 2023, CISA and 17 U.S. and international partners published an update to a joint Secure by Design white paper on "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software." Originally released April 13, 2023, this paper urges software manufacturers to revamp their design and development programs to produce only secure by design products. It also emphasizes three core principles: 1.) Take ownership of customer security outcomes, 2.) Embrace radical transparency and accountability, and 3.) Lead from the top.



- **Leading on Artificial Intelligence.** CISA published its first Roadmap for Artificial Intelligence (AI) in November 2023, adding to the significant U.S. Department of Homeland Security and broader whole-of-government effort to ensure the secure development and implementation of AI capabilities. This Roadmap outlines a whole-of-agency plan to assess possible cyber-related risks to the use of AI, provide guidance to the critical infrastructure sectors that Americans rely on every hour of every day, and capitalize on AI's potential to improve U.S. cyber defenses.

- **Reducing the Risk of Ransomware.** In March 2023, CISA launched the Pre-Ransomware Notification Initiative, which measurably reduces risk by warning organizations of early-stage ransomware activity. Since the Initiative's launch, the agency conducted more than 1,000 pre-ransomware notifications across a variety of critical infrastructure sectors and to partners abroad.

- **Encouraging Cyber Hygiene.** In September 2023, CISA launched its Secure Our World program. Secure Our World is a new and enduring cybersecurity awareness program that emphasizes four simple cyber hygiene steps everyone should implement and continuously improve upon: 1.) Use Strong Passwords and a Password Manager, 2.) Turn On Multifactor Authentication, 3.) Recognize and Report Phishing, and 4.) Update Software. The campaign featured CISA's first-ever public service announcement (PSA) And garnered significant public attention through outreach efforts including television, radio and billboard ads,

podcasts, media coverage, social media and beyond.

- **Supporting Critical Infrastructure.** CISA enhanced its engagement with "target rich, resource poor" organizations, including the Water and Wastewater Sector, K-12 Education Subsector, Healthcare and Public Health Sector and the Election Security Sector. In 2023, CISA completed more than 6,700 stakeholder engagements with government and private sector participants to share threat information and promote its cybersecurity services.

- **Enhancing Emergency Communications.** In 2023, CISA accumulated new subscribers to CISA's Priority Telecommunication Services (PTS) program which enables essential personnel to communicate when landline or wireless networks become degraded, congested or otherwise unavailable. The PTS program covers wireline communications under Government Emergency Telecommunications Service (GETS), wireless voice communications under Wireless Priority Service (WPS), and priority repair and installation of critical voice and data circuits under Telecommunications Service Priority (TSP). In 2023, GETS added 51,023 new subscribers, thanks in large part to focused outreach during the second annual Emergency Communications Month in April. In addition, WPS users increased by 283,357 subscribers. TSP also added restoration priority to 18,307 new circuits that support national security emergency preparedness missions.

- **Providing Resources to State and Local Governments.** In 2023,

CISA and the Federal Emergency Management Agency (FEMA) jointly implemented the State and Local Cybersecurity Grant Program (SLCGP). The SLCGP is a first-of-its-kind cybersecurity grant program specifically for state, local and territorial governments across the country. In September 2023, CISA and FEMA announced the of Notice of Funding Opportunity for the Tribal Cybersecurity Grant Program, allocating \$18.2 million to bolster cybersecurity among federally-recognized tribes.

- **Strengthening Regional Election Security Support.** In 2023, CISA established dedicated election security advisors (ESAs) in each of its 10 regions to provide support and resources to promote secure elections. These ESAs work directly for CISA's Regional Directors and with the agency's cybersecurity and protective security advisors to ensure CISA's capabilities and services are being optimally employed to meet the unique needs of each state or locality.

- **Improving Security for Chemical Facilities.** CISA celebrated the second anniversary of its ChemLock voluntary program in November 2023. This program provides facilities possessing dangerous chemicals with tailored, scalable, no-cost services and tools to improve their chemical cyber and physical security posture.

This digitally interactive 2023 Year in Review takes on a new look and feel, providing the reader with a brief snapshot of CISA's accomplishments while linking back to corresponding CISA.gov webpages for a deeper dive into its programs and initiatives.

## CISA and ENISA enhance their Cooperation

The European Union Agency for Cybersecurity (ENISA) has signed a Working Arrangement with the Cybersecurity and Infrastructure Security Agency (CISA) of the US, in the areas of capacity-building, best practices exchange and boosting situational awareness. Geopolitics have shaped the cyber threat landscape, bringing like-minded partners closer together in the wake of common cyber challenges and advances in digital technologies. Today at the EU-US Cyber Dialogue, ENISA and CISA announced the signing of their Working Arrangement as an important milestone in the overall cooperation between the United States and the European Union in the field of cybersecurity, also following the Joint Statement of European Commissioner Thierry Breton and U.S. Secretary for Homeland Security Alejandro Mayorkas of January 2023.

ENISA's International Strategy directs the Agency to be selective in engaging with international partners and to limit its overall approach in international cooperation to those areas and activities that will have high and measurable added value in achieving the Agency's strategic



objectives. CISA is a key partner to ENISA in achieving these objectives and by extension the EU in achieving a higher common level of cybersecurity. The Working Arrangement is both a consolidation of present areas of cooperation, as well as opening the door to new ones. Current examples are the organisation and promotion of the International Cybersecurity Challenge (ICC), exchanging best practices in the area of incident reporting or ad hoc information exchanges on basic cyber threats.

### Signing partners:

CISA leads the United States' effort to understand, manage, and reduce risk to cyber and physical infrastructure. "In today's highly complex and borderless cyber threat landscape, collaboration remains key to everything we do," said CISA Director Jen Easterly. "CISA's Working

Arrangement with ENISA signifies a new chapter in our collective resilience. Together we will enhance cybersecurity awareness, fortify capacity building initiatives, and foster a robust environment for knowledge sharing and best practice exchanges, ensuring a safer digital landscape for our citizens."

European Union Agency for Cybersecurity (ENISA), Executive Director, Juhan Lepasaar, said: "This new Working Arrangement is an evolution and consolidation of the effective cooperation with our US counterpart. The structured collaboration will address some of our common challenges in the cyber threat landscape."

This arrangement is broad in nature and covers both short-term structured cooperation actions, as well as paving the way for longer-term cooperation in cybersecurity policies and implementation approaches. Cooperation

will be sought in the areas of:

- Cyber Awareness & Capacity Building to enhance cyber resilience: including facilitating the participation as third country representatives in specific EU-wide cybersecurity exercises or trainings and the sharing and promotion of cyber awareness tools and programmes.
  - Best practice exchange in the implementation of cyber legislation; including on key cyber legislation implementation such as the NIS Directive, incident reporting, vulnerabilities management and the approach to sectors such as telecommunications and energy.
  - Knowledge and information sharing to increase common situational awareness: including a more systematic sharing of knowledge and information in relation to the cybersecurity threat landscape to increase the common situational awareness to the stakeholders and communities and in full respect of data protection requirements.
- A work plan will operationalise the Working Arrangement and regular reporting at the EU-US Cyber Dialogues is foreseen.

## CISA Issues Request For Information on Secure by Design Software Whitepaper

the Cybersecurity and Infrastructure Security Agency (CISA) published a Request for Information from all interested parties on secure by design software practices, including the Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software whitepaper, as part of our ongoing, collective secure by design campaign across the globe.

To better inform CISA's Secure by Design campaign, CISA and our partners seek information on a wide range of topics, including the following:

- Incorporating security early into the software development life cycle (SDLC): What changes are needed to allow software

manufacturers to build and maintain software that is secure by design, including smaller software manufacturers? How do companies measure the dollar cost of defects in their SDLC?

- Security is often relegated to be an elective in education: What are some examples of higher education incorporating foundational security knowledge into their computer science curricula; When new graduates look for jobs, do companies evaluate security skills, knowledge, and experience during the hiring stage, or are employees reskilled after being hired?
- Recurring vulnerabilities: What are barriers to eliminating recurring classes

of vulnerability; how can we lead more companies to identify and invest in eliminating recurring vulnerabilities; how could the common vulnerabilities and exposures (CVE) and common weakness enumeration (CWE) programs help?

- Operational technology (OT): What incentives would likely lead customers to increase their demand for security features; Which OT products or companies have implemented some of the core tenants of secure by design engineering?
- Economics of secure by design: What are the costs to implement secure by design and default principles and tactics, and how do these compare to costs responding to incidents and breaches?

"While we have already received a wide range of feedback on our secure by design campaign, we need to incorporate the broadest possible range of perspectives," said CISA Director Jen Easterly. Our goal to drive toward a future where technology is safe and secure by design requires action by every technology manufacturer and clear demand by every customer, which in turn requires us to rigorously seek and incorporate input. The President's National Cybersecurity Strategy calls for a fundamental shift in responsibility for security from the customer to software manufacturers, and input from this RFI will help us define our path ahead, including updates to our joint seal Secure by Design whitepaper.

## CISA Releases Key Risk and Vulnerability Findings for Healthcare and Public Health Sector

The Cybersecurity and Infrastructure Security Agency (CISA) published a Cybersecurity Advisory (CSA), Enhancing Cyber Resilience: Insights from the CISA Healthcare and Public Health Sector Risk and Vulnerability Assessment, detailing the agency's key findings and activities during a Risk and Vulnerability Assessment (RVA) conducted at a healthcare and public health (HPH) organization in early 2023. The advisory also provides network defenders

and software manufacturers recommendations for improving their organizations' and customers' cyber posture, which reduces the impact of follow-on activity after initial access.

The CISA assessments team identified several findings as potentially exploitable vulnerabilities that could compromise the confidentiality, integrity, and availability of the tested environment. Tailored for HPH organizations of all

sizes as well as for all critical infrastructure organizations, the advisory provides several recommended mitigations mapped to 16 specific cybersecurity weaknesses identified during the RVA. Also, the advisory provides three mitigation strategies that all organizations should implement: (1) Asset

management and security, (2) Identity management and device security, and (3) Vulnerability, patch, and configuration management. Each strategy has specific focus areas with details and steps on how HPH entities can implement them to strengthen their cybersecurity posture.



**CISA**  
CYBER+INFRASTRUCTURE



# Help2Protect against the Insider Threat

## Insider Threat Awareness and Program Development Training platform

### Help2Protect.info

Protect your company from Insider Threats

In Collaboration  
with:



See below for  
20% Off Special  
Offer

### THREE TYPES OF INSIDERS - ONE TOOL TO DETECT THEM

Insiders may be involuntarily helping by not being sufficiently aware and trained about the potential impact of their actions, or they may be negligent. Only a small proportion of Insiders are malicious and have the intentional aim to damage the organisation. The Help2Protect program covers all 3 categories of Insiders: accidental, negligent and malicious. It also includes all types of crimes, including theft, espionage, sabotage, violent activism and organised crime, including terrorism.

### BE PROACTIVE AWARENESS TRAINING



How to help to protect you, your  
organisation and your colleagues.

### BE READY PROGRAM DEVELOPMENT TRAINING



How do you develop an effective Insider  
Threat Program for your organisation

An eLearning Platform dedicated  
to Security and the Insider Threat

[www.help2protect.info](http://www.help2protect.info)

**SPECIAL OFFER FOR IACIPP – 20% DISCOUNT OFF THE COURSE**

IACIPP are offering you a 20% discount off this Insider Threat Detection and Prevention online course.

Register at: [www.cip-associaion.org/help2protect](http://www.cip-associaion.org/help2protect) - Promo Code: 7UATQW7M

## Mobile Access from Bosch uses smartphones instead of plastic cards

Thanks to Mobile Access, the new solution from Bosch, access to buildings and restricted areas can now be managed without additional identification media such as plastic cards.



Mobile Access is fully integrated into the tried-and-tested Access Management System from Bosch and offers numerous benefits in terms of efficiency, security, and convenience for building owners, employees, and visitors.

A few clicks are all it takes for authorized individuals, such as Facility Management or IT staff, to configure and create access authorizations in their local Access Management System. Visitor and employee data can then be managed with ease using an intuitive, browser-based interface.

Mobile Access leverages the Bosch Group's many years of experience with products and systems in the field of security, safety, and communications. The new solution modernizes access control without

compromising on high security standards. Mobile Access uses forgery-proof certificates to transmit authorization credentials via BLE (Bluetooth Low Energy) between the smartphone and the reader and employs the encrypted OSDP protocol between the reader and controller.

The solution also supports two-factor authentication that can be configured on the readers. Visitors and employees are then prompted to unlock their smartphone to gain access, for instance by using their Face ID. This makes it especially easy to comply with strict data protection laws, because sensitive personal data does not have to be stored on local systems. That means building operators also benefit from secure and cost-effective two-factor authentication.

## HID Enhances Its PKI Offerings with Acquisition of Trusted Certificate Service Provider ZeroSSL

HID, a worldwide leader in trusted identity solutions, announces the acquisition of ZeroSSL, an SSL certificate provider based in Austria.



The acquisition will not only augment HID's capabilities in providing protected communications to and from websites, but also strengthen its reputation as a leading provider of trusted PKI solutions.

"This acquisition marks another step in expanding our PKI and IoT business," said Martin Ladstaetter, HID Senior VP and Managing Director for IAMS. "Bringing ZeroSSL's established expertise and strong brand into the HID portfolio reinforces our commitment to safeguarding digital transactions while expanding our suite of offerings."

SSL certificates create an encrypted connection between a web server and a browser, safeguarding data privacy. Issuing more than 500,000 monthly certificates

to more than 2.4 million user accounts globally, ZeroSSL's robust offerings include an automated e-commerce platform for SSL certificates and integration services for lifecycle management of those certificates. Without such automation, website operators and owners must manually manage the SSL certificate, thereby risking outages due to human errors and ensuing cybersecurity risks.

Moving forward, ZeroSSL's offerings will be integrated into HID's PKI and IoT Business Unit, allowing HID to be better positioned to provide even stronger authentication, better encryption services, and more comprehensive validation procedures for organizations engaging in large-scale online transactions.



## Johnson Controls Shows How Artificial Intelligence, IoT, Cloud Computing Rapidly Transforming the Future of Smart Buildings

The pressure to meet global climate targets has never been greater and with buildings accounting for 40% of global greenhouse gas emissions, there is an urgent need to advance sustainable building technology to help enterprises meet net zero goals while accommodating for continued growth.



“The Smart Building of the Future,” a new paper from Johnson Controls outlines how smart buildings equipped with advanced technologies like artificial intelligence, IoT, cloud and cybersecurity will help enterprises create a future where our buildings integrate with human and environmental ecosystems. Smart buildings offer a harmonized environment that prioritizes both well-being and sustainability, using technology to adapt and unlock potential, support productivity and drive peak performance of building occupants.

Several factors are converging to accelerate the development and adoption of advanced building systems technology. As building owners work to respond to challenges

such as rising energy costs and changes in occupancy patterns, among others, sophisticated IoT devices and the implementation of data analytics and AI have become more important than ever.

The report also offers building managers key insights into the major technology enablers of advanced smart buildings, including: Ubiquitous connectivity through cloud-based services; AI-enabled autonomous smart buildings; Digital twins enable a continuous feedback loop between the physical and the virtual by facilitating the integration of AI, IoT and cloud technologies to generate strategic recommendations for improving building performance and user experience.

## Axis Communications Completes Integration of ASSA ABLOY Aperio® Wireless Technology into the AXIS Camera Station Secure Entry Platform

ASSA ABLOY Opening Solutions announces that Axis Communications, an industry leader in video surveillance, access control, intercom, and audio systems, has completed the integration of ASSA ABLOY Aperio® wireless lock technology into the AXIS Camera Station Secure Entry all-in-one video and access control management system.



Aperio is a global wireless platform that works with extensive locking hardware options from ASSA ABLOY Group brands, offering the flexibility to address a variety of applications throughout any facility. The platform uses wireless communication (IEEE 802.15.4) between the lock and an Aperio hub to provide real-time communication to the access control system, simplifying installation and reducing costs.

AXIS Camera Station Secure Entry offers secure, scalable, and unified access control. It is a complete access control solution that combines physical access control with video verification for easy monitoring, assistance, and investigations. It allows

facilities to secure entrances, grant and assign access, and understand who is going where and when.

“This collaboration with ASSA ABLOY promises simplicity and cost-effectiveness, eliminating cumbersome installations and budget constraints. It offers a streamlined, efficient way to expand access control capabilities, making security upgrades accessible to more organizations. Moreover, real-time online communication between Aperio® locks and AXIS Camera Station Secure Entry ensures enhanced security and efficiency,” states Rob Druktenis, Program Manager, Access Control at Axis Communications.



## XProtect 2023 R3 boosts efficiency, collaboration, and system control

Milestone Systems, a leading provider of video technology, announces the release of XProtect 2023 R3, the latest version of its highly scalable, flexible, data-driven video management software (VMS).



This update builds on XProtect's leading open platform technology with new capabilities that increase operational efficiency, enhance collaboration, and provide tighter system control.

New XProtect 2023 R3 key features:

**Onboarding Feature Guide:** This built-in feature in the Web Client presents operators with information on how the Web Client is structured. This helps operators be more efficient, making onboarding of new employees easier and faster;

**Role-Based Alarm Notifications:** Users can now create alarm notification profiles that route alerts to specific operators based on their function. This prevents alarm fatigue by only sending relevant alarms to each user and helps

operators focus on what really matters. Response times improve by putting critical alerts immediately in the right hands.

In addition to these top new features, the 2023 R3 update contains a wide array of other enhancements, including cybersecurity hardening, improved VMS resilience, and expanded integrations with third-party systems via XProtect's open API architecture.

The 2023 R3 release continues Milestone's commitment to pushing the boundaries of open-platform video technologies. The company's focus on innovation ensures that XProtect users always have access to the latest capabilities to maximize the value of their video infrastructure.

## Darktrace and Garland Technology Collaborate to Help Businesses Secure Operational Technology Environments

Darktrace, a global leader in cyber security AI, and Garland Technology, a leading manufacturer of network TAP (test access point), aggregator, packet broker, data diode and inline bypass solutions, announced a new collaboration to help businesses protect complex industrial environments.

Security risks in industrial environments and critical infrastructure continue to rise. The increasing monetization of OT attacks, exposure of Industrial Control Systems (ICS) to open networks, and convergence with IT is heightening opportunities for threat actors. The number of industrial IoT (IIoT) devices is increasing rapidly, with the global number of industrial IoT connections forecasted to reach 37 billion in 2025 according to Juniper Research, creating entry points for adversaries and leaving major visibility gaps for security teams who are already faced with tight budgets and personnel shortages.


Together, Garland's Network TAPs and Aggregators and Darktrace/OT are designed to quickly enable visibility and security across OT, IT, and IIoT networks to Purdue level 1. Purdue level 1 includes devices, such as programmable logic controllers (PLCs) and remote terminal units (RTUs) that sit closest to the physical industrial processes. Using Garland's network TAP solutions with Darktrace

minimizes deployment challenges with little to no additional configuration required in complex industrial environments, quickly illuminates points of IT and OT convergence, provides unidirectional traffic flow, and detects potential threats to keep data and environments secure.

Darktrace/OT uses Self-Learning AI to learn every detail of an organization's bespoke OT systems, delivering increased visibility and detecting subtle deviations to stop threats at their earliest stages.

Garland Technology's network TAP solutions create a foundation of visibility for network management, allowing secure access and monitoring of network traffic. Garland's solutions are uniquely designed for industrial networks.

This collaboration brings Darktrace/OT™ and Garland Technology's network visibility solutions together, offering fast, seamless deployments and more complete network visibility in operational technology (OT) environments.



**critical infrastructure**  
PROTECTION AND  
RESILIENCE **N. AMERICA**  
March 12<sup>th</sup>-14<sup>th</sup>, 2024  
L'Auberge Hotel & Casino  
LAKE CHARLES, LOUISIANA, USA  
A Homeland Security Event

**Securing the Inter-Connected Society**  
For Securing Critical Infrastructure and Safer Cities



**World Border Security Congress**  
24<sup>TH</sup>-26<sup>TH</sup> APRIL 2024  
ISTANBUL, TURKEY  
[www.world-border-congress.com](http://www.world-border-congress.com)



**critical infrastructure**  
PROTECTION AND  
RESILIENCE EUROPE  
12<sup>th</sup>-14<sup>th</sup> NOV 2024  
Madrid, Spain  
[www.cipre-expo.com](http://www.cipre-expo.com)

## ADVERTISING SALES

Ray Beauchamp -  
Americas  
E: [rayb@torchmarketing.co.uk](mailto:rayb@torchmarketing.co.uk)  
T: +1-408-921-2932

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

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

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





**24<sup>TH</sup>-26<sup>TH</sup> APRIL 2024**  
**ISTANBUL, TURKEY**

[www.world-border-congress.com](http://www.world-border-congress.com)

## Where East Meets West - Developing Border Strategies Through Co-operation and Technology

### INVITATION TO ATTEND - REGISTER ONLINE TODAY

You are invited to attend the 2024 World Border Security Congress  
Register online at [www.world-border-congress.com/registration](http://www.world-border-congress.com/registration)

Turkey is a transcontinental country, strategic positioned linking Europe, Asia and the Middle East, making it a perfect route for trade.

With a total border boundary of some 4,000 miles, about three-quarters is maritime, including coastlines along the Black Sea, the Aegean, and the Mediterranean, as well as the narrows that link the Black and Aegean seas.

The 'EU-Turkey deal', a 'statement of cooperation' between EU states and the Turkish Government, means Turkey can take any measures necessary to stop people travelling irregularly from Turkey to the Greek islands, and currently manages over 5 million migrants and refugees.

Turkey is a top destination for victims of human trafficking, as well a global trafficking hub for South American cocaine, fuelling rising demand for the drug in Eastern Europe and the Persian Gulf.

Many challenges face the region, which impacts globally, and therefore, an excellent place for the hosting of the next World Border Security Congress.

The World Border Security Congress is a high level 3 day event that will discuss and debate current and future policies, implementation issues and challenges as well as new and developing technologies that contribute towards safe and secure border and migration management.

We look forward to welcoming you to Istanbul, Turkey on 24th-26th April 2024 for the next gathering of border and migration management professionals.

[www.world-border-congress.com](http://www.world-border-congress.com)

*for the international border management and security industry*

#### CONFIRMED SPEAKERS INCLUDE:

- AEAC Diane Sabatino, Acting Executive Assistant Commissioner (AEAC) for the Office of Field Operations (OFO), US CBP
- Amanda Read, National Operational lead, Safeguarding & Modern Slavery, UK Border Force
- Ana Cristina Jorge, Director of Operational Response Division of the European Border and Coast Guard Agency – Frontex
- Austin Gould, Assistant Administrator for Requirements and Capabilities Analysis, Transport Security Administration
- Colleen Ryan, Border Advisor, Border Security & Management Unit, Transnational Threats Department (TNTD), OSCE
- Dr Maria Carmela Emanuele, Customs Officer - Chemist, Italian Customs and Monopolies Agency
- Emmanuel Oshoba, Deputy Comptroller of Customs, Nigeria Customs Service
- Guido Ferraro, Project Manager, Joint Research Centre, European Commission
- Iliuta Cumpanasu, Lead Evaluator, FRONTEX
- LTC Marcos Pérez-Mayor Rodríguez, Chief of Staff of the Border and Customs Police Command, Guardia Civil, Spain

Full Speakers at [www.world-border-congress.com/speakers](http://www.world-border-congress.com/speakers)

Supported by:

Media Partners:

