critical infrastructure PROTECTION AND RESILIENCE NEWS

Official Magazine of

International Association of CIP Professionals

WINTER 2022/23
www.cip-association.org

FEATURE:
Government and Industry Cooperation: More Important Than Ever for Cybersecurity Awareness

FEATURE:
Can responsible AI guidelines keep up with the technology?

FEATURE:
An Interview with Port of New Orleans

critical infrastructure PROTECTION AND RESILIENCE AMERICAS
7th-9th March 2023
Baton Rouge, LA, USA
Preliminary Event Guide inside

A STANDARD TO HELP PROTECT CRITICAL INFRASTRUCTURE

critical infrastructure PROTECTION AND RESILIENCE AMERICAS

March 7th-9th, 2023

BATON ROUGE, LOUISIANA

A Homeland Security Event

Co-Hosted and Supported by:

International Association of CIP Professionals

INFRAGARD MEMBERS ALLIANCE LOUISIANA

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

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 protrection 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 Sector Symposium
- Transport Sector Symposium
- Communications Sector Symposium
- CBRNE Sector Symposium
- Critical Manufacturing & Logistics Sector Symposium
- Government, Defence & Space Sector Symposium

Join us in Baton Rouge, 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

Opening Keynotes:

- Dr David Mussington, Assistant Director, CISA
- Clay Rives, MPA, LEM-P, Director, East Baton Rouge Mayor's Office of Homeland Security & Emergency Preparedness

Confirmed speakers include:

- Richard Tenney, Senior Advisor, Cyber, CISA Emergency Communications Division, CISA
- Vanessa Tibbits, Special Officer In Charge, FBI
- Jill Farria, Supervisory Transportation Security Inspector, TSA
- Dr Ashley Pennington, Chemical Engineer CISA
- Douglas DeLancey, Chief, Strategy Branch, Office for Bombing Prevention
- Lester Millet, Safety Agency Risk Manager / FSO Workgroup Chairman, Port of South Louisiana & Infragard Louisiana President
- Colleen Wright, Priority Telecommunications Area Representatives, CISA
- Leigh J. Blackburn, Ph.D., Senior IT Specialist, Program Manager for Secure Tomorrow Series, CISA
- Charles Burton, Technology Director, Calcasieu Parish Government
- Sunny Wescott, Lead Meteorologist - Extreme Weather Outreach, CISA
- Dawn Manga, Associate Director Priority Communications, CISA
- Jeff Gaynor, President, American Resilience
- Ron Martin, Professor Of Practice, Critical Infrastructure, Capitol Technology University

For speaker line-up visit www.ciprna-expo.com

REGISTER ONLINE AT www.ciprna-expo.com/registration

WELCOME TO CRITICAL INFRASTRUCTURE PROTECTION AND RESILIENCE

Welcome to the latest Critical Infrastructure Protection and Resilience News, the official magazine of the International Association of Critical Infrastructure Protection Professionals (IACIPP).

IACIPP is a non-profit organisation that provides a platform for sharing good practices, innovation and insights from Industry leaders and operators alongside academia and government and law enforcement agencies. At the heart of our association, we strongly believe in the power of a collaborative community where individuals/organisations and agencies can openly share their knowledge and experiences to increase visibility and recognition of issues and learning.

The last few years have not been the easiest of times. The Covid-19 pandemic dominated 2020 and 2021 and just as we all thought we were entering calmer times Russia invaded Ukraine, starting a war in Europe. As a consequence, 2022 was an extremely challenging year. We saw the threat of tactical nuclear weapons, energy price hikes, inflation rates reaching their highest point for over 40 years and the spiralling cost of living impacting on everyone.

It is impossible to predict the future but the one constant is change and 2023 will, I am sure, continue to be both challenging and complex in ways that we can reasonably expect and quite possibly in ways that we had not foreseen nor planned for.

If the world continues to be challenging and complex then you can bet your bottom dollar that the issues impacting critical infrastructure will continue to deliver more complexity and uncertainty.

Critical infrastructure is crucial to modern life, it spans everything from healthcare, water and education to chemicals, transportation, and energy systems not to mention broadband, telecoms and other vital systems. It underpins all the critical functions that keep our nations and our economies running and unfortunately it continues to face a wide range of threats and challenges.

Those within and with an interest in, the industry, understand the range of threats that are to be addressed, from weather related events to the physical security and resilience issues and of course the escalation of cyber-attacks.

Some recent research (Check Point Research) has found that global cyber-attacks increased by 28% in the third quarter of 2022 compared to the same

www.cip-association.org

Editorial:
Neil Walker
E: neilw@torchmarketing.co.uk

Design, Marketing & Production:
Neil Walker
E: 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.

TORCH

period in 2021 and a significant percentage of that increase has been focused on our infrastructure.

Cyberattacks will continue to target critical infrastructures such as health systems, government agencies and educational institutions and ransomware remains a popular attack method for all targets, no matter their size.

We have only really just started to understand the full impact of insufficient cybersecurity being in place. While governments and regulators increase their pressure on organisations to demonstrate that their plans and preparations are effective and fit for purpose, it has become increasingly evident that the current ways of managing cyber risks and information security compliance, as a whole, need weighty levels of investment and research if they are to keep up to speed with the pace and complexity of both current and future attack activities.

Governments across the globe are increasingly conscious of the potential negative societal impact should any of their critical national infrastructure be affected by any type of event, be it natural or man-made. In November 2022 President Biden announced his attention for the administration to "review and revise, as appropriate" the nation's foundational policy on critical infrastructure, Presidential Policy Directive 21 (PPD 21). This is seen as an important moment in homeland security, as presidential policy has long been the driver for defining the fundamental relationship between government and industry in managing risk.

We have seen similar activities across a number of countries where action has been delivered around the "review and revise" process leading to some noteworthy benefits. Benefits such as, a greater level of cooperation and communication across countries, with joint messaging being produced to evidence effective levels of collaboration. We have also seen substantial levels of investment into those agencies with responsibility for the protection of infrastructure, in particular around cyber security with CISA in the USA and the NCSC in the UK, being prime examples.

I am a strong believer in collaboration, cooperation and communication being the drivers for new learning and the effective management of the threats that our infrastructure has to contend with. This is not just limited to cross government and cross industry action. It is about all who have a part to play, an interest in and a story to tell around the protection and resilience of our critical infrastructure.

The IACIPP looks forward to events such as the Critical Infrastructure Protection and Resilience North America Conference as it brings like minded people together to discuss the issues of the day and to share both individual and organisational learning experiences.

I am fortunate, to once again have the honour to Chair this event, which is taking place in Baton Rouge, Louisiana between the 7th and 9th March this year. The agenda has an amazing line up of speakers and looks set to be an event not to be missed. I look forward to seeing you there.

John Donlon QPM FSyI
IACIPP Chairman

Collaborating and Cooperating for Greater Security
critical infrastructure
PROTECTION AND RESILIENCE AMERICAS
7th-9th MAR 2023
Baton Rouge, LA, USA
A Homeland Security Event
For Securing Critical Infrastructure and Safer Cities

World Border Security Congress
25TH-27TH APRIL 2023
SKOPJE, NORTH MACEDONIA (BALKANS)
www.world-border-congress.com
BORDER PATROL
EMERGENCY EXIT

ADVERTISING SALES

Jina Lawrencec
UK & ROW
E: jinal@torchmarketing.co.uk
T: +44 (0) 7958 234750

Sam Most
Mainland Europe &Turkey
E: samm@torchmarketing.co.uk
T: +44 (0) 208 123 7909

Ray Beauchamp
Americas
E: rayb@torchmarketing.co.uk
T: +1-559-310-0330

A Standard to help protect Critical Infrastructure

By Catherine Piana, Director General of CoESS

Protecting Critical Infrastructure against malicious attacks has never been higher a priority. Threats are becoming more complex and varied, including terrorism from political groups or Nation States, activists and, more recently, as a result of the war in Ukraine. The private security industry is very conscious of the role it plays in this context and is contributing to the legislative and standardization effort at EU level. While the CER Directive is in the final stages of adoption, the CEN Standard System for Private Security Services in Critical Infrastructure Protection is being built. Here's how the two will function together.

About CoESS

Let me first introduce the organization I represent: the Confederation of European Security Services, in short CoESS. We speak on behalf of the private security industry in Europe. This industry employs over 2 million security officers, which is the same number as police officers in the same region. Our organization is a recognized Social Partner and this is important because, together with UNI Europa, we stand for quality in this labour-intensive industry. Quality means well selected, trained, and motivated staff. Quality is achieved by complying with regulations, collective agreements and standards, offering a safe environment to the staff, clients and the general public. Ultimately, the combination of quality, compliance and safety converges towards an essential value in this security environment, namely trust.

How do our values translate into reality?

In order to make these values a reality to ensure the resilience of Critical Entities, we have four different avenues that are complementary:

- Adequate legislation;
- Good procurement practices;
- Use of recognized standards;
- Public-private partnerships.

Let me take these one by one.

Adequate legislation: CoESS has been working together with the EU Institutions on its future legislation for the Resilience of Critical Entities – the CER Directive. Our main points were to ensure that private security companies and staff would meet quality criteria, including the right level of training, and that CI operators could select these companies according to industry-recognised standards. The final text of the Directive enshrines these principles, which is an excellent outcome of our efforts. The next step will be to make reinforce these principles at national level, while the Directive is being transposed into National Law. Our member National Associations have the opportunity to use the Directive's margin for maneuver to transform these recommendations into obligations.

Good procurement practices: it may come as a surprise to the laymen, but still too many contracts for security CI are focused mainly on the price and much less on quality. This may not be an issue on an everyday basis, and it's mainly when CI operators will need robust services in times of crisis, attacks or in ensuring business continuity that they will find out that cheap also means lousy quality. The cost of an incident gone wrong on the CI's reputation and business continuity will in every case be much higher than that of going for quality in the first place. While there is legislation on public procurement transposed from the EU Directive 2014/24/EU, it is quite lax in some countries. For this reason, CoESS has produced a guide for buyers of private security services, to help them through the procurement process, public or private. "Buying Quality Private Security Services" can be downloaded in 15 languages here.

I will come to the use of standards more extensively in the next paragraph, as they are a crucial element today with the new CER Directive.

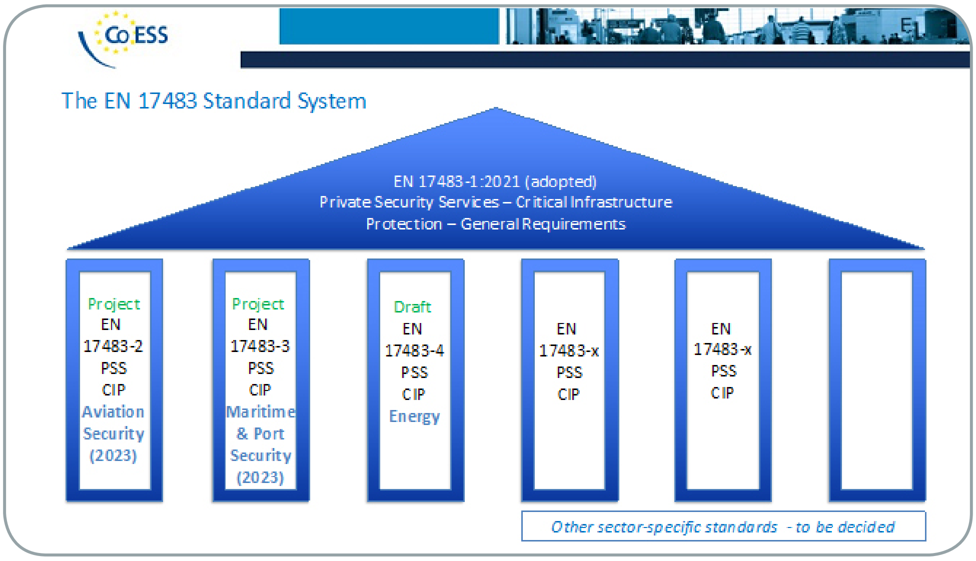
Last but not least, having efficient and effective Public-Private Partnerships (PPPs) to secure CI is also very important. CoESS wrote a White Paper on the Security Continuum, which elaborates on existing Best Practice in PPPs in 5 different countries and in various locations (not just in CI) to draw recommendations for successful PPPs. Among these, we find again a mention to best value procurement, but also what PPPs should cover to establish mutual understanding between the parties and lead them towards the same goal. Finally it touches on the need to raise the level of security awareness, culture, and training, including on the Insider Threat.

The strategic dimension of standards

The word "standard" is not a very attractive one and it generates all sorts of mental representations. It is not often associated with the word "strategy", although there is an essential strategic dimension to standards if it is used as a business enabling tool. Let me explain: if, as we tried to achieve in our work on the CER Directive, clients have to select their providers among compliant or, better still, certified companies, this creates a very strategic dimension for standards.

How does this work?

Standards are in their vast majority voluntary but if there is a pull effect from clients, then they are no longer optional. This is what we are seeking to create by combining the CER Directive's "recommendation" to use standards, with the quality criteria established in CEN standards. Within the CEN Technical Committee (TC) 439 "Private Security Services", which I



The EN 17483 Standard System

EN 17483-1:2021 (adopted)
Private Security Services – Critical Infrastructure Protection – General Requirements

Project EN 17483-2 PSS CIP Aviation Security (2023)

Project EN 17483-3 PSS CIP Maritime & Port Security (2023)

Draft EN 17483-4 PSS CIP Energy

EN 17483-x PSS CIP

EN 17483-x PSS CIP

Other sector-specific standards - to be decided

International Association of
CIP Professionals
www.cip-association.org

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 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 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

chair, we have been working since 2016 on creating a whole "standards system". With this system, we establish the quality criteria for private security companies that protect CI. The first standard, which is the foundation of the system is EN 17483-1:2021 "Private Security Services – Critical Infrastructure Protection – General Requirements". It covers the criteria for the provider, contracts, staff and service delivery. The next standards will cover, one by one, all areas of CI that require it, starting with the current projects prEN17483-2 for Aviation and Airports, prEN17483-3 for Maritime and Ports Security and the future EN17483-4 for Energy Production and Transmission. Companies wishing to deliver security services, for example in an Airport, will have to be compliant (or better still, certified) to both the General Requirements EN 17483-1 and the aviation-specific standard EN 17483-2. The sector-specific standards mainly cover training requirements and quality control.

If you are a buyer of those services, think about this: if companies don't comply with these objective and measurable criteria, remember that this is just the visible part of the iceberg. Just imagine what is going on in the part you cannot see and think about what may happen in a crisis – any type of crisis.

The tools are there for you to use!

Critical Infrastructure come in all shapes and sizes. Some are run by private companies, some are public. But they all are essential to the functioning of our societies. The interdependencies between them are significant and require adequate protection by companies that show compliance with quality criteria. The threats are numerous from simple sabotage to espionage, from theft to penetration by organized crime including terrorism and through physical means, cyber-attacks or combined attacks. The tools are there to select the right partners to protect them so feel free to use them!

In summary

- Critical infrastructure is what is most essential to the functioning of our economies and democracies
- Security is not a commodity, it is an enabler
- Private Security Companies can be the trusted partner of Law Enforcement Agencies and CI operators
- There are objective ways to distinguish legitimate and professional PSCs from the "others"
- Standards are an objective way to do choose quality and best value
- The standard system EN 17483-1 helps select quality private security services to protect Critical Infrastructure

Critical Infrastructure: Actions Needed to Better Secure Internet-Connected Devices

The USA's 16 critical infrastructure sectors rely on internet-connected devices and systems to deliver essential services, such as electricity and health care. These sectors face increasing cybersecurity threats—an issue on our High Risk list.

Federal agencies that have leadership roles in 3 sectors we reviewed have taken some steps to manage the cybersecurity risks posed by internet-connected devices and systems. But they've not assessed risks to the sectors as a whole. Without a holistic assessment, the agencies can't know what additional cybersecurity protections might be needed.

Cyber threats to critical infrastructure IoT and OT represent a significant national security challenge. Recent incidents—such as the ransomware attacks targeting health care and essential services during the COVID-19 pandemic—illustrate the cyber threats facing the nation's critical infrastructure. Congress included provisions in the IoT Cybersecurity Improvement Act of 2020 for GAO to report on IoT and OT cybersecurity efforts.

This report (1) describes overall federal IoT and OT cybersecurity initiatives; (2) assesses actions of selected federal agencies with a lead sector responsibility for enhancing IoT and OT cybersecurity; and (3) identifies leading guidance for addressing IoT cybersecurity and determines the status of OMB's process for waiving cybersecurity requirements for IoT devices. To describe overall initiatives, GAO analyzed pertinent guidance and related documentation from several federal agencies.

To assess lead agency actions, GAO first identified the six critical infrastructure sectors considered to have the greatest risk of cyber compromise. From these six, GAO then selected for review three sectors that had extensive use of IoT and OT devices and systems. The three sectors were energy, healthcare and public health, and transportation systems. For each of these, GAO analyzed documentation, interviewed sector officials, and compared lead agency actions to federal requirements.

GAO also analyzed documentation, interviewed officials from the selected sectors, and compared those sector's cybersecurity efforts to federal requirements. GAO also interviewed OMB officials on the status of the mandated waiver process.

Government and Industry Cooperation: More Important Than Ever for Cybersecurity Awareness

by Chuck Brooks, President, Brooks Consulting International

With another National Cybersecurity Awareness Month upon us, few major things have changed from the past year in terms of threats. As the capabilities and connectivity of cyber devices have grown, so have the cyber intrusions from malware and hackers. The cyber- threat actor ecosystem has grown in both size and sophistication. They are also openly collaborating in sharing targets. And tools. The cyber threat actors include various criminal enterprises, loosely affiliated hackers, and adversarial nation states.

Information sharing on threats and risk is one of the most principal functions of government and industry collaboration.

Achieving a full awareness of nefarious actors who operate in the cyber realm and protecting against their capabilities is an arduous task. Clearly, industry cannot respond to growing cyber-threats alone, especially for small and medium businesses who lack the resources and expertise. Increased government and industry cooperation to meet those challenges is a viable course to help mitigate threats and challenges. It is a proven risk management model that makes good sense. In several areas.

Information sharing on threats and risk is one of the most principal functions of government and industry collaboration. Sharing such information helps allow both government and industry to keep abreast of the latest viruses, malware, phishing threats, ransomware, and insider threats. Information sharing also establishes working protocols for lessons-learned and resilience that is critical for the success of commerce and the enforcement against cyber-crimes.

Both Solar Winds and the Colonial pipeline breaches highlighted the government's assistance in mitigating breaches and moving toward resilience. Government was directly collaborating with the companies to discover the extent of the breaches and options for amelioration.

Remediation of breaches is important to continuity; no matter what, breaches will happen. The incorporation of best practices and the lessons learned from the various and many corporate breaches over the past few years is certainly valuable data for both industry and government in terms of prevention, recovery, and continuity.

Government Takes Proactuve Role With Industry Partnerships

The government and industry partnership is being well coordinated via the Cybersecurity and Infrastructure Protection Agency (CISA) of the Department of Homeland Security (DHS). Over the past few years, CISA has taken on a formal and increasingly larger role as the lead civilian agency in government working with industry, and state & local and tribal stakeholders on cybersecurity threats. The proposed 2023 DHS budget has appropriated more than $2.5 billion toward cybersecurity demonstrating the importance of the agency's role in protecting the homeland in cyberspace, including in the aforementioned areas of information sharing and resilience.

Most significant is that CISA under the leadership of Jen Esterly created the Joint Cyber Defense Collaborative (JCDC) last year to fundamentally transform how cyber risk is reduced through continuous operational collaboration between government and trusted industry partners. "The Cybersecurity and Infrastructure Security Agency established JCDC—the Joint Cyber Defense Collaborative—to unify cyber defenders from organizations worldwide. This diverse team proactively gathers, analyzes, and shares actionable cyber risk information to enable synchronized, holistic cybersecurity planning, cyber defense, and response." The JCDC also is supported by other government agencies including the FBI, NSA, and U.S. Cyber Command to help drive down risk in partnership with industry.

In recent years, DHS along with The National Institute of Standards (NIST), has made a growing effort to bring the private sector together with the government, especially to develop information sharing protocols in risk management. In a core sense, a successful cyber threat consequences strategy is really about risk mitigation and incident response. A risk management strategy requires stepping up assessing situational awareness, information sharing, and especially resilience planning. It is critical to be aware of the morphing threat landscape and plan contingencies for all potential

scenarios. NIST has been extremely helpful to industry in those areas.

The White House has also heighted government and industry cooperation in various areas including supply chain security, protecting critical infrastructure (most of which is owned by the private sector). In specific regard to critical infrastructure, the underlying goal of collaboration is to help protect against targeted cyber intrusions of the nation's critical infrastructure, such as financial systems, chemical plants, water and electric utilities, hospitals, communication networks, commercial and critical manufacturing, pipelines, shipping, dams, bridges, highways, and buildings.

White House and industry cooperation has been primarily aimed at identifying vulnerabilities, ensuring security, and integrating resilience in the public/private cyber ecosystem. The most recent activity by the White House was an executive order formulating a Zero trust strategy for government agencies. That "trust nothing connected" perspective is also being assimilated in industry.

Congress has supported CISA's expanded role and involvement with industry. Several bi-partisan bills have bolstered the agency's integral role in cyber preparedness, response and resilience for both government and industry.

Cooperative Research and Development

Research and development of potentially disruptive cybersecurity technologies is another benefit of government and industry cooperation. The change in the cyber risk environment coinciding with a heightened need for procurement of innovative technologies and services has created a new paradigm for a cybersecurity partnership between government and industry.

Together, government and the private sector can identify products and align flexible product paths, evaluate technology gaps, and help design scalable architectures that will lead to more efficiencies, and fiscal accountability. Bridging R&D spending between the government and private sectors should also allow for a more directed and capable cybersecurity prototype pipeline to meet modern technology requirements.

An enhanced and streamlined government and industry partnership should continue to be a priority for cybersecurity strategies in 2023, as threats can morph, especially with the emergence of technologies such as artificial intelligence, machine learning, 5G, and eventually quantum computing. The partnership needs to be both proactive and adaptive to change as the threat matrix may become increasingly lethal to economic and strategic stability if we remain unaware and unprepared for the potential consequences.

Trends in maritime communications

An estimated 90 per cent of the goods traded around the world travel by sea. Vital commodity flows, as well as seafarer safety, hinge on ever more sophisticated maritime communication networks.

Much of the world's commerce would simply not be possible without the plethora of technologies making up today's maritime communications ecosystem. These include ship stations (meaning radiocommunication equipment on board commercial, passenger or patrol vessels, etc.); coast stations that support ships at sea; as well as radar services, automatic identification, and maritime distress systems.

Although the International Maritime Organization (IMO) develops regulations for shipping, ensuring safe maritime communication largely falls to the International Telecommunication Union.

ITU Recommendations, Reports, Regulations, and databases – along with giving seafarers vital information – help safeguard the frequency bands that vessels use to navigate safely, as explained by ITU's German Medici.

Modernizing the GMDSS

Distress, safety, and emergency maritime communications are coordinated through the Global Maritime Distress and Safety System (GMDSS), which uses terrestrial communication and satellite systems (such as those operated by Inmarsat and Iridium) to connect ships and coast stations. Discussions currently underway at ITU aim to make the GMDSS more flexible in terms of maritime safety information distribution, which in turn should open the door to new technology applications in this area, said Medici.

The GMDSS continues to evolve to improve and enhance maritime communications and safety. Satellite EPIRBs operating at 1.6 gigahertz (GHz) and using very high frequency (VHF) systems for DSC will no longer be part of the GMDSS. However, the IMO may soon allow an existing geostationary satellite system to become a new GMDSS satellite service provider, explained Medici.

Evolving e-navigation

In the future, seafarers will increasingly rely on communications services, such as e-navigation, which IMO defines as "the harmonized collection, integration, exchange, presentation and analysis of marine information on board and ashore by electronic means to enhance berth-to-berth navigation and related services for safety and security at sea and to protect the marine environment". High-speed broadband connections will keep ships and shore facilities continuously updated and let mariners follow real-time data displays on the bridge.

Ships will increasingly use VHF data exchange systems that integrate data exchange, application-specific messaging, and automatic identification capabilities in the same VHF maritime band, Medici added.

Beacon detection and response

Cospas-Sarsat, a satellite-aided, treaty-based search and rescue initiative that has been operational since 1985, is now developing a second-generation beacon and medium-Earth orbit search and rescue system (MEOSAR), in which repeaters are placed on global navigation satellite system (GNSS) satellites.

The initiative brings together 45 nations and agencies to collaboratively detect and locate radio beacons activated by aircraft, vessels or people in distress.

This Cospas-Sarsat development will enable near-time global coverage of beacon localization and distress message transmission, said Medici. A new "return-link-service" (RLS) will give users a confirmation that their message was received.

Autonomous vessels on the waves

Maritime autonomous surface ships (MASS) are also on the horizon. These are ships that can operate independently (to varying degrees) of human interaction.

"In April 2022, IMO began work on the development of a regulatory framework for Maritime Autonomous Surface Ships," Medici noted. The work aims to integrate new and advancing technologies in its regulatory framework – balancing the benefits derived from new and advancing technologies against safety and security concerns, the impact on the environment and on international trade facilitation, the potential costs to the industry, and their impact on personnel, both on board and ashore.

For the moment, these "autonomous vessels" lack specified spectrum requirements. But that may change as MASS communications requirements are identified. "The development of MASS may be supported by future ITU studies, including potential determination of their spectrum needs, and the publication of associated ITU Recommendations and Reports," Medici concluded.

Help2Protect against the Insider Threat

Insider Threat Awareness and Program Development Training platform

In Collaboration with:

International Association of CIP Professionals

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

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-association.org/help2protect - Promo Code: 7UATQW7M

Help2Protect: an eLearning program to counter Insider Threats

By Catherine Piana, Managing Director of Help2Protect SRL

There are only 2 ways to know if you are being targeted by Insiders: one is to wait for an actual breach of security to happen and the other is to have a program in place that detects Insider Threats and protects against them. Help2Protect is an eLearning Platform dedicated to Security and the Insider Threat courses help you put in place a detection and prevention program against this widespread and yet largely underestimated issue.

A few facts and figures

In the US only, businesses encounter about 2,500 internal security breaches daily. More than 34% of businesses around the globe are affected by Insider Threats yearly and it is estimated that the number of Insider incidents has increased by 44% in the last two years. 66% of organizations consider malicious Insider attacks or accidental breaches more likely than external attacks. The cost per Insider Threat in 2022 is over 15 million USD. Statistics further reveal that more than 70% of attacks are not reported externally. Up to a quarter of these attacks are perpetrated by trusted business partners .

You don't know until it's too late

Most organisations discover Insider Threats when it's too late, while programs exist that can help prevent and detect them, and thereby protect the organisation, its people, assets, infrastructure and reputation. Help2Protect provides 2 streams of training: a very accessible and simple awareness module (30' on average) and a thorough set of 7 modules, and downloadable template material to create a complete Insider Threat prevention and detection program from the ground up.

It starts with trust

Any organisation may be the target of Insider Threats but Critical Infrastructure are regularly targeted and the impact may be significant not just to the people and infrastructure, but to society as a whole. During Covid19 and even more since the war in Ukraine, attacks have also included a cyber dimension, most of the time supported by human actions that allow these attacks to be carried out.

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.

Let's talk about you!

Is your organisation ready to detect and prevent Insider Threats? At which stage of preparation are you and your staff? Does your staff know how to identify red flags, and when, how and to whom they should report them? Do you know how to set up an Insider Threat Program? These are some of the issues that the updated Help2Protect platform will help you address.

Help2Protect will also show you how you can set up an Insider Threat Detection and Prevention Team, including all the relevant departments of your organisation that need to be involved, including Human Resources, Finance, IT, Legal and Security. We take you through the main steps of the process, so you can start protecting your employees, your assets, your customers, your infrastructure, and your reputation.

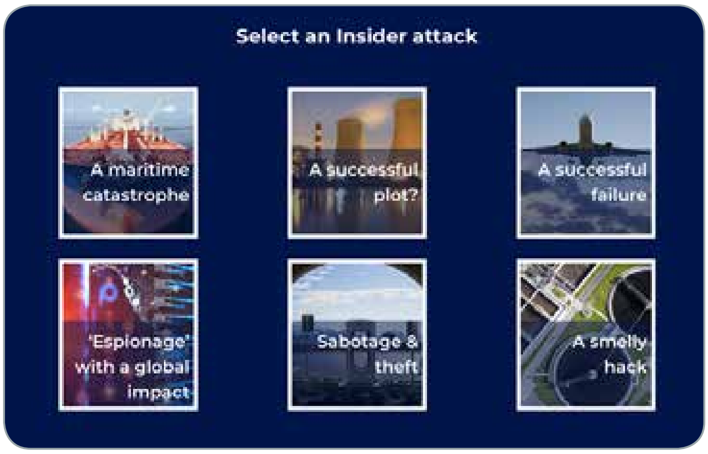
The 2 modules

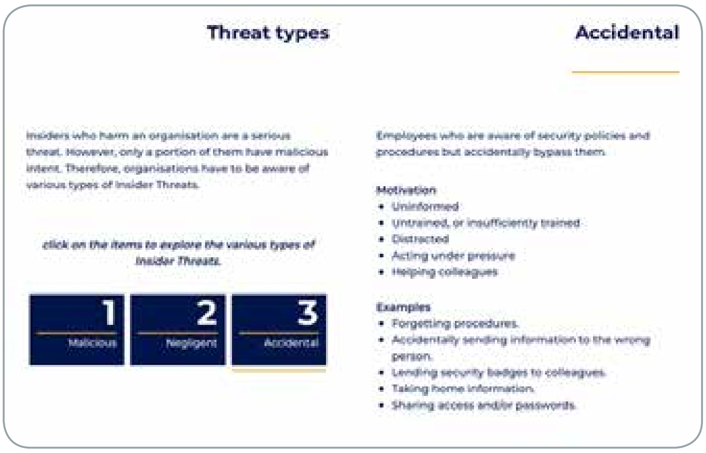
- The Awareness Module (AM) is for any member of your staff, whatever their level of education or skillset. It seeks to explain how the organisation may be targeted, what types of behaviours and red-flag actions should raise their attention. By explaining the potential consequences of Insider attacks on the staff and the organization, it encourages them to report actions and behaviours that are deviating from what one might expect in a normal situation. To make this very concrete, six actual cases are briefly introduced, and the actions that should have been taken to prevent them. This Module takes participants about 30 minutes to complete. They then take a quiz and download their personalised certificate.

- The Program Development Module (PDM): includes 7 modules and a Manual, as well as a toolbox of template documents. The complete set of 7 modules takes about 3 hours to complete. The Manual serves as a "learning companion" and can be downloaded. The modules address the following themes:

o Demonstrating the Return on Investment of an Insider Threat Program

o Going into detail of 6 Insider Threat cases and explaining the Insider's motivations, profiles and the pathway to malicious action or behaviour – including the





Threat types

Insiders who harm an organisation are a serious threat. However, only a portion of them have malicious intent. Therefore, organisations have to be aware of various types of Insider Threats.

click on the items to explore the various types of Insider Threats.

Accidental

Employees who are aware of security policies and procedures but accidentally bypass them.

Motivation

- Uninformed
- Untrained, or insufficiently trained
- Distracted
- Acting under pressure
- Helping colleagues

Examples

- Forgetting procedures.
- Accidentally sending information to the wrong person.
- Lending security badges to colleagues.
- Taking home information.
- Sharing access and/or passwords.

windows for detection

o Understanding various Insider Threat models and how they can be identified before it's too late

o Building an Insider Threat Prevention team: criteria and success factors

o Guidelines for safe hiring from an HR perspective

o How to communicate about the Insider Threat policy within the organisation

o Best practices from experts who have gone through actual Insider Threat cases

How was the platform created?

Help2Protect is a spin-off of an EU-funded project (DG HOME Internal Security Fund), called AITRAP. During the 2-year project, the companies involved, namely Securitas, DHL, Palmyra Aviation Advisors and the Confederation of European Security Services, carried out a meta-analysis of all the literature and tools on Insider Threats and created this unique e-learning platform with the support of a specialized e-learning company in the Netherlands, called Splintt.
The project Manager and Coordinator made sure that the platform would be financed for 3 years but at the end of this period (end 2021), it had to close down. They then decided to take it over, review it and update it. Help2Protect became a joint venture between them. At the moment, the platform only provides courses on Insider Threats but it will in the future include more modules, for example on how to build a security culture.

What is special about Help2Protect?

The team that took over are security practitioners who are closely and daily in touch with EU and International security organisations and decision-makers. They use their field experience to make the modules rich and real. They also have a deep understanding of and experience in the human psychology, as well as training and coaching experience.

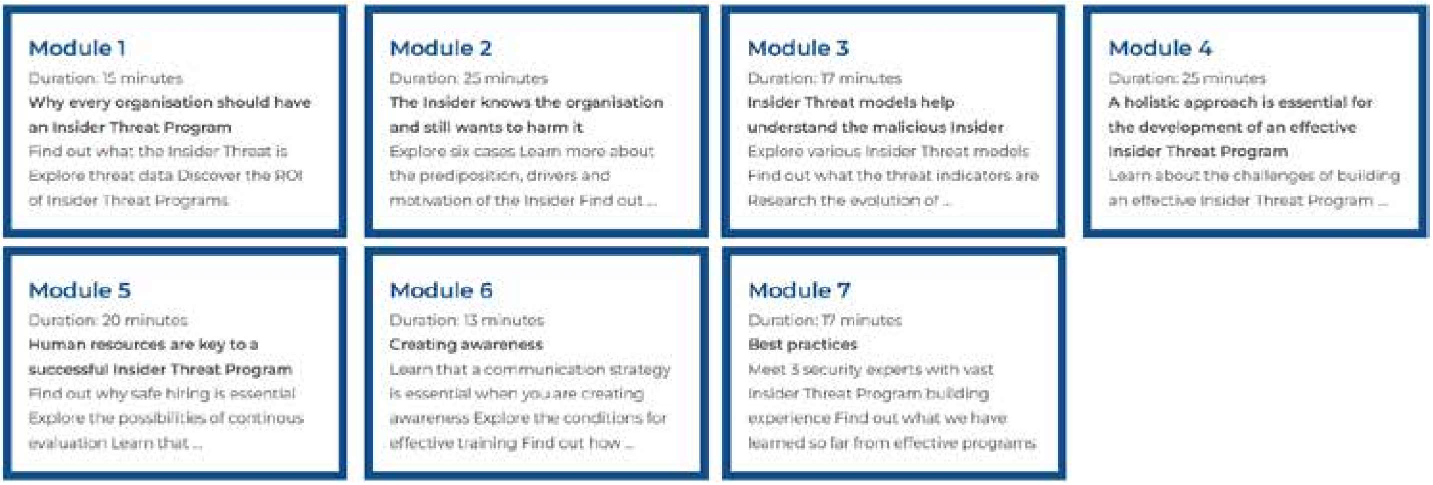
Follow us on Twitter: https://twitter.com/Help2Protect

Follow us on LinkedIn: https://www.linkedin.com/company/help2protect

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-association.org/help2protect - Promo Code: 7UATQW7M



Module 1
Duration: 15 minutes
Why every organisation should have an Insider Threat Program
Find out what the Insider Threat is Explore threat data Discover the ROI of Insider Threat Programs

Module 2
Duration: 25 minutes
The Insider knows the organisation and still wants to harm it
Explore six cases Learn more about the predisposition, drivers and motivation of the Insider Find out ...

Module 3
Duration: 17 minutes
Insider Threat models help understand the malicious Insider
Explore various Insider Threat models Find out what the threat indicators are Research the evolution of ...

Module 4
Duration: 25 minutes
A holistic approach is essential for the development of an effective Insider Threat Program
Learn about the challenges of building an effective Insider Threat Program ...

Module 5
Duration: 20 minutes
Human resources are key to a successful Insider Threat Program
Find out why safe hiring is essential Explore the possibilities of continous evaluation Learn that ...

Module 6
Duration: 13 minutes
Creating awareness
Learn that a communication strategy is essential when you are creating awareness Explore the conditions for effective training Find out how ...

Module 7
Duration: 17 minutes
Best practices
Meet 3 security experts with vast Insider Threat Program building experience Find out what we have learned so far from effective programs

Protecting essential infrastructure: MEP approve deal on new rules with broader scope

Parliament and EU member states' negotiators have agreed on new rules to make the EU's essential infrastructure more resilient.

Negotiating teams from the European Parliament and the Council of the EU reached a deal on the resilience of essential infrastructure. The new rules would establish harmonised minimum rules to ensure that different member states classify the same providers as essential, and risk assessments for essential infrastructure to boost its resilience in the face of disruptions and hazards. The scope would be expanded to eleven sectors in total, including energy, transport, banking, financial market infrastructures, health, drinking water, waste water, food, digital infrastructure and space. At Parliament's request, public administration was also included in the scope of the rules.

Under the new rules, critical service-providers would have to carry out risk assessments of their own and report disruptive incidents. Also, Member States would be required to adopt national strategies for boosting resilience and carry out regular risk assessments. National authorities should have the possibility to conduct on-site inspections of critical infrastructure, and introduce penalties in case of non-compliance.

To harmonise communication, each member state should designate a single point of contact to act as liaison and ensure functioning cross-border cooperation.

MEPs pushed for broader scope

In the negotiations, MEPs wished to widen the definition of essential services to also include the environment and public health and safety, which were adopted. They also managed to include consideration of rule of law in the context of resilience against threats and risks. The directive will therefore also address possible threats affecting the functioning of national systems that safeguard the rule of law.

To smoothen cross-border co-operation, MEPs wanted to lower the threshold of recognising service providers as having "European significance". In the end, it was agreed that the threshold be lowered from ten or more member states (in the Commission proposal) to six or more, which will cover several hundreds of critical entities of the European significance across the Union. At the same time, MEPs wanted to ensure coherence between the present directive and the NIS2 directive on cybersecurity.

After the vote, rapporteur Michal Šimečka (Renew, SK) said: "Against the backdrop of the pandemic and Russia's war in Ukraine, securing Europe's critical infrastructure has become a top priority. Today's agreement will boost the resilience of critical entities, and as the Parliament's lead negotiator, I pushed to include in the scope of the regulation new and vital sectors, including food production and distribution and public administration. I'm also satisfied that we retained a key provision that will allow Member States to develop a common understanding of what services are essential in any crisis scenario. We, as the Parliament, must not let fragmentation and divergence in national rules stand to weaken the resilience of European societies from increasingly frequent physical and hybrid threats."

Background

In the previous directive on critical infrastructures, only energy and transport were within the scope of common rules. The European Parliament called for the revision of previous directive in a resolution on the findings of the Special Committee on Terrorism in 2018. On 16 December 2020, the European Commission published its proposal for a new directive on the resilience of critical entities.

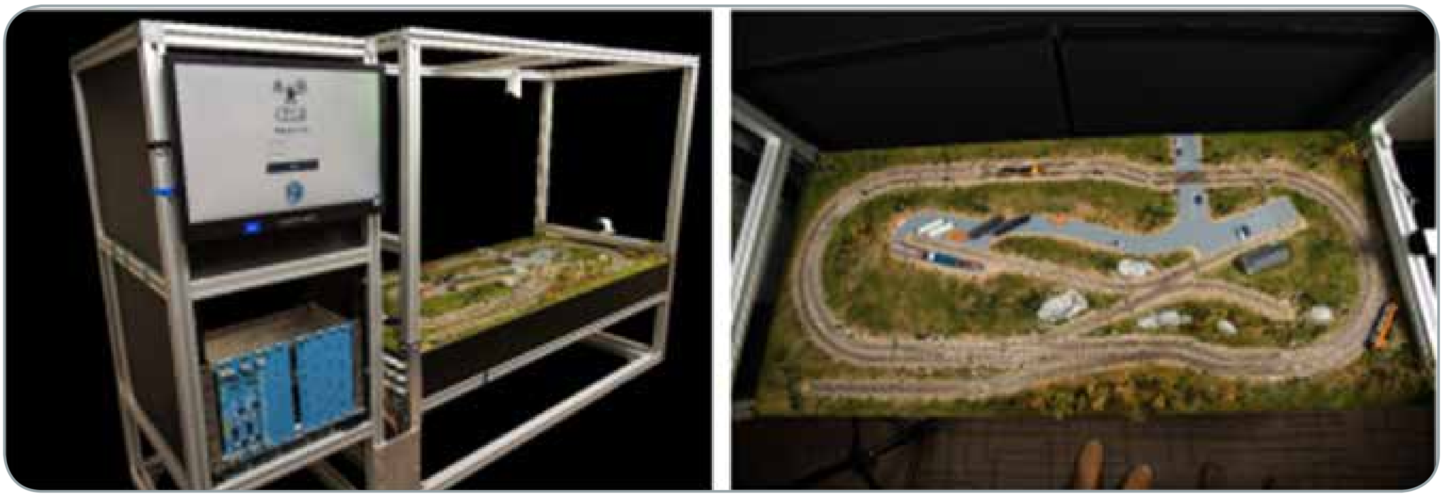
Testing Environments Help S&T and CISA Secure Transportation Infrastructure

Catherine Piana, Chairperson of TC439 and Director General of CoESS

Strengthening and protecting our nation's critical cyber infrastructure is a monumental task, one that the Science and Technology Directorate (S&T) takes seriously. Together with the Cybersecurity and Infrastructure Security Agency (CISA), S&T is developing and testing new technologies and tools that will help combat daily threats, both physical and online.

"All critical infrastructure sectors—including the energy, manufacturing, and transportation sectors—rely heavily on sophisticated technologies like industrial control systems, cellular networks, and artificial intelligence," said S&T program manager Alex Karr. "These are all accessed, monitored, and controlled via the internet, which, in turn, makes them susceptible to hacking, malware attacks, and other malicious activities."

Our critical infrastructure and associated online networks and technologies play a vital role in



PNNL's rail test environment will serve as a valuable tool to help prepare rail industry experts for potential cyberattacks against our nation's rail infrastructure. Photo credit: PNNL.

ensuring that the most essential services of our government and private sectors can do their job. Because of this, any potential weaknesses that can be exploited, disrupted, or damaged represent a significant threat to the safety of our citizens and our country. "This is why it's crucial that we do everything we can to boost our online security and make sure we're ready to respond to any attempts to compromise these crucial services and related systems," Karr said.

S&T is working with a multi-agency team to do just that, collaborating with CISA, the Idaho National Laboratory (INL), Pacific Northwest National Laboratory (PNNL), and other government and private stakeholders to design and implement two state-of-the-art training tools, both a part of CISA's Control Environment Laboratory Resource (CELR) test environment. These CELR test environments, one designed by INL and the other by PNNL, will eventually be integrated into CISA's existing suite of internet security tools.

"CELR test environments are miniaturized test environments that emulate crucial facilities and their associated technologies and physical components," explained Tim Huddleston, INL program manager for Infrastructure Assurance and Analysis. "They are designed to provide first responders and security professionals with a safe setting to simulate cyberattacks, conduct research on and analysis of these attacks, and practice the implementation of countermeasures that will enable them to detect, mitigate, or prevent such incidents in the real world."

"S&T, CISA, INL and PNNL currently operate six CELR test environments: a chemical processing plant; an electric distribution substation; an electric transmission substation; a natural gas compressor station; a building automation system; and a water treatment facility," explained Karr. "And recently, we've identified the need to develop additional training and testing tools for our transportation sector, which is why we are working with INL, PNNL and subject matter experts in this field to build and implement two new cutting-edge automotive and rail test environments."

Thanks to a new partnership with the auto industry, S&T, CISA, and INL have procured a state-of-the-art electric, semi-autonomous car and are converting it into an automotive testbed that will host cybersecurity incident response training, research, and analysis on this increasingly utilized class of energy-efficient, "smart" vehicles.

"This test environment will provide CISA staff, automotive manufacturers, and transportation security experts with a tool to help them gain a better understanding of electric semi-autonomous vehicles, their communications systems, control units and other electrical and physical components, and the ways that these systems and components can potentially impact other drivers and vehicles that share our roads," explained CISA's branch chief of Industrial Control Systems Section, Alex Reniers. "It will also help them discover whether or not these vehicle technologies—such as over the air maintenance, safety sensors, Bluetooth capabilities, key fobs, payment systems, and charging station ports—can be accessed and hacked for malicious purposes."

Any potential IT vulnerabilities

that are discovered during the development and implementation of the automotive test environment will promptly be shared with the auto industry in order to help them develop appropriate security measures that can be deployed in future models of their energy-efficient, "smart" vehicles.

"Semi-autonomous electric vehicles and their associated technology and infrastructure requirements represent a significant and ongoing evolution in the world of automotive transportation," said Reniers. "And we want to ensure the safe development and rollout of these vehicles as they become more popular and widely available to consumers everywhere."

In addition to the automotive test environment, S&T, CISA, and PNNL are also working with rail transportation subject matter experts to develop a similar CELR test environment that will provide CISA, other internet security professionals, and rail operators and manufacturers with a tool that enables them to better understand, manage, and reduce the possibility and effects of successful hacking and cyber-physical attacks aimed at our trains and associated infrastructure.

Chemical security experts call for multisector cooperation against terrorism

The devastating impact of chemical weapons and explosives used in acts of terrorism continues to affect civilian populations and is well known for its destructive and long-term harm.

Last year over 1,000 improvised explosive device (IED) attacks were conducted by non-state actors, injuring over 7,150 people in more than 40 countries. Many attacks come from chemicals that criminals acquired through weak points in the supply chain – from manufacturing to storage and retail– and made into weapons.

To counter this threat, some 220 chemical security practitioners from more than 70 countries met at INTERPOL's 3rd Global Congress on Chemical Security and Emerging Threats to find ways of reducing vulnerabilities by enhancing multisector cooperation and collaboration.

With a focus on acquisition, transportation, physical and cyber security of chemical materials, the meeting highlighted a range of security issues, such as detecting cross-border movements of regulated material and implementing regulatory frameworks.

Terrorists' misuse of e-commerce and new technologies

The Global Congress also explored ways to counter emerging threats including terrorists' misuse of e-commerce and new technologies to acquire toxic and precursor chemicals.

Due to the substantial growth and access to the Internet in recent years, so too we have seen an increase in digital content produced and shared through platforms such as instant messaging, social networking, blogs and online portals. The misuse of technologies can be seen as a result of this rapid growth in content, and with it a rise in suspicious activities.

Law enforcement agencies provided examples of investigative techniques that could be used to identify and prosecute the illicit purchase or sale of chemicals on the Dark Net. These lessons provided delegates with solutions to address the use of sophisticated technologies for nefarious purposes.

"The concerted effort of global law enforcement, along with our partners, is key to combatting the use of explosive precursor chemicals and chemical weapons," Mr Hinds added.

Dual-use and precursor chemicals have a wide legitimate function in the production of consumer goods such as pharmaceuticals, cleaning supplies and fertilizers. This raises significant challenges to prevent and monitor, and remains one of the inherent threats to chemical security worldwide.

INTERPOL awareness video - 'The Watchmaker'

In this context, an INTERPOL-produced awareness video was premiered at the meeting to engage a broad spectrum of stakeholders in understanding the importance of individuals and companies to secure dangerous toxic chemicals, including equipment.

Entitled 'The Watchmaker', the video highlights the need for multisector cooperation to combat these threats and will be used in a series of INTERPOL capacity building workshops and other activities related to counter-terrorism and prevention.

"Multisector collaboration is essential for us to tackle the threats we face from criminals who gain access to dangerous chemicals with malevolent intentions. Morocco is committed to strengthening the engagement of these issues as part of our proactive approach to combating terrorism," said Mr. Mohammed Dkhissi, Head of National Central Bureau, Rabat.

Can responsible AI guidelines keep up with the technology?

As artificial intelligence (AI) technology continues advancing at lighting pace, discussions on the need for governance, standards, and a stronger focus on "responsible AI" have followed.

While AI can carry out decision-making tasks efficient, it's still based on algorithms that respond to data models. Unlike humans, AI algorithms can't see the full picture, in part because they lack emotional reasoning and other human qualities, such as empathy, ethics, and morality.

Concerns over privacy and discrimination are on the rise as AI becomes further integrated into decision-making processes that affect economies and societies worldwide.

The time has come, therefore, to decide what sort of policies should guide AI design and use, and how to make sure AI use improves human welfare and respects human dignity, said Nashlie Sephus, Principal Tech Evangelist for Amazon AI, in a recent AI For Good keynote.

According to AI Principles put forward by the Organisation for Economic Co-operation and Development (OECD), responsible AI is "innovative and trustworthy" and "respects human rights and democratic values."

Sephus describes six dimensions of

responsible AI: privacy and security; fairness; explainability; robustness; transparency; and governance.

The main hindrance to making AI responsible in practice, she adds, is the need to focus on a few priorities while keeping up with new innovations.

"It can be a challenge to figure out how we can do responsible AI in practice when you have so many different use cases and technologies being released every day," she said. "We also want to make sure that we're covering all our bases, so there's a lot at stake here. As innovation continues to move so fast, responsible AI should move just as fast, if not faster."

Setting priorities for responsible AI

For Sephus, "safety of life" technologies in healthcare, law enforcement, and transport should be tackled first.

She also advises companies to focus on one problem at a time, depending on their technology's use case: "It really pays to understand the total environment that your system is going to be deployed in, and how that environment may or may not change over time."

The varied, case-by-case nature of responsible AI, however, will continue making it hard to implement.

"Everything is use-case specific," said Sephus. "The way you define success or fairness metrics depends on what you're doing. Sometimes you have systems that do multiple things, so making sure you define your bias evaluation for every single feature your system encompasses is crucial."

Questions about the root cause of bias in AI outputs add another layer of complexity.

Standards and governance needed

Governments play an important role in implementing responsible AI, especially when it comes to high-risk, life-or-death use cases. "For example, an autonomous vehicle system can actually put someone's life at risk," Sephus noted. "We want to make sure that governments are prioritizing the things that are really critical at this moment."

Asked about the most urgent legal issue around AI, she responded: "The challenge is the government figuring out how to reign in and capture everything that's going on. How do they make this applicable across the board? From computer vision to language processing to recommendation systems – each has nuances in it that you may or may not be able to correct for if it's already out there."

One way governments can increase accountability in AI is through documentation, which is tied closely to accountability.

"We must hold people accountable by putting systems and mechanisms in place that will enforce these things, not just say them and leave it to the technologists to govern themselves," Sephus said.

Education is another key driver of accountability, making ethics courses an essential part of any well-rounded AI curricula. "When people know better, they do better," said Sephus. "Let's create standards on a global scale to help educate people. That can happen at the university level, but it can start as early as high school."

Yet access to AI remains relatively exclusive in today's world.Many communities still lack access to the Internet, let alone AI platforms. In effect, the poorest and most vulnerable segments of humanity are also being left behind in this most transformative aspect of digital economies and societies.

"A lot of the time, these are target groups who are impacted by the lack of responsible AI," Sephus explained. "It's important for us to recognize and include those people."

Making the AI community more diverse is one way to foster inclusion, she added. "A more diverse generation of leaders in machine learning is crucial. As the industry heads in this direction, we should do a better job at training more diverse populations, and large industries have a responsibility to contribute to that."

Responsible AI by design

During a live Q&A session, AI for Good participants asked how start-ups with scarce resources can prioritize responsible AI from the very beginning, such as by building it into their product or service design.

"Start-up life is very competitive," answered Sephus, advising AI-adopting businesses to "tell your investors, customers and stakeholders" about the benefits. "I guarantee you 100 per cent that will put you ahead compared to your competitors."

Amazon Web Services provides a range of tools to help its customers practice responsible AI. Sagemaker Groundtruth, for example, helps customers label their data and improve their overall data quality through the training and integration of human annotators.

Watch the full keynote:

While AI tools can assist with problem-solving, achieving responsible AI still requires human collaboration, Sephus concluded. "While I'm in the AI industry and know that it has many capabilities, it still cannot replace two humans talking and collectively reaching an accord to figure out how they can solve a problem."

By ITU News

CISA Developed Cross-Sector Recommendations to Help Organizations Prioritize Cybersecurity Investments

The Department of Homeland Security released the Cybersecurity Performance Goals (CPGs), voluntary practices that outline the highest-priority baseline measures businesses and critical infrastructure owners of all sizes can take to protect themselves against cyber threats. The CPGs were developed by DHS, through the Cybersecurity and Infrastructure Security Agency (CISA), at the direction of the White House. Over the past year, CISA worked with hundreds of public and private sector partners and analyzed years of data to identify the key challenges that leave our nation at unacceptable risk. By clearly outlining measurable goals based on easily understandable criteria such as cost, complexity, and impact, the CPGs were designed to be applicable to organizations of all sizes. This effort is part of the Biden-Harris Administration's ongoing work to ensure the security of the critical infrastructure and reduce our escalating national cyber risk.

"Organizations across the country increasingly understand that cybersecurity risk is not only a fundamental business challenge but also presents a threat to our national security and economic prosperity," said Secretary of Homeland Security Alejandro N. Mayorkas. "The new Cybersecurity Performance Goals will help organizations decide how to leverage their cybersecurity investments with confidence that the measures they take will make a material impact on protecting their business and safeguarding our country."

CISA developed the CPGs in close partnership with the National Institute for Standards and Technology (NIST). The resulting CPGs are intended to be implemented in concert with the NIST Cybersecurity Framework. Every organization should use the NIST Cybersecurity Framework to develop a rigorous, comprehensive cybersecurity program. The CPGs prescribe an abridged subset of actions – a kind of "QuickStart guide" – for the NIST CSF to help organizations prioritize their security investments.

"To reduce risk to the infrastructure and supply chains that Americans rely on every day, we must have a set of baseline cybersecurity goals that are consistent across all critical infrastructure sectors," said CISA Director Jen Easterly. "CISA has created such a set of cybersecurity performance goals to address medium-to-high impact cybersecurity risks to our critical infrastructure. For months, we've been gathering input from our partners across the public and private sectors to put together a set of concrete actions that critical infrastructure owners can take to drive down risk to their systems, networks and data. We look forward to seeing these goals implemented over the coming years and to receiving additional feedback on how we can improve future versions to most effectively reduce cybersecurity risk to our country."

"Given the myriad serious cybersecurity risks our nation faces, NIST looks forward to continuing to work with industry and government organizations to help them achieve these performance goals," said Under Secretary of Commerce for Standards and Technology and NIST Director Laurie E. Locascio. "Our priority remains bringing together the right stakeholders to further develop standards, guidelines and practices to help manage and reduce cybersecurity risk."

Infrastructure Resilience Planning Framework (IRPF)

The Cybersecurity and Infrastructure Security Agency (CISA) has developed the Infrastructure Resilience Planning Framework (IRPF) to enable the incorporation of security and resilience considerations in critical infrastructure planning and investment decisions.

Infrastructure is the backbone of our communities, providing not only critical services (such as water, transportation, electricity, and communications), but also the means for health, safety, and economic growth. These systems often extend beyond our communities providing service to entire regions and contributing to the delivery of National Critical Functions. Given the vital importance of infrastructure to our social and economic well-being, it is imperative we ensure our networks are strong, secure, and resilient. In order for communities to thrive in the face of uncontrollable circumstances and adapt to changing conditions (e.g., evolving security threats, impacts from extreme weather, technological development, and socio-economic shifts), we must work to make our infrastructure more resilient.

Presidential Policy Directive 21 (PPD-21) – Critical Infrastructure Security and Resilience defines resilience as the ability to prepare for and adapt to changing conditions and withstand and

recover rapidly from disruptions. Infrastructure resilience depends on both physical attributes of engineered infrastructure systems and on the capabilities of organizations affecting the operation and management of those systems (e.g., infrastructure owners and operators, regulatory authorities, and vendors and contractors). Resilience is also influenced by organizational factors such as the existence of business continuity and emergency response plans, the level of workforce training, and the frequency of exercises to test plans. Developing resilience is essential to managing the wide range of risks that communities face, including those presented by dependencies between and among infrastructure systems.

The Cybersecurity and Infrastructure Security Agency (CISA) developed the Infrastructure Resilience Planning Framework (IRPF) to provide an approach for localities, regions, and the private sector to work together to plan for the security and resilience of critical infrastructure services in the face of multiple threats and changes. The primary audience for the IRPF is state, local, tribal, and territorial governments and associated regional organizations; however, the IRPF can be flexibly used by any organization seeking to enhance their resilience planning. It provides resources for integrating critical infrastructure into planning as well as a framework for working regionally and across systems and jurisdictions.

This framework provides methods and resources to address critical infrastructure security and resilience through planning, by helping communities and regions:

> Understand and communicate how infrastructure resilience contributes to community resilience;

> Identify how threats and hazards might impact the normal functioning of community infrastructure and delivery of services;

> Prepare governments, owners and operators to withstand and adapt to evolving threats and hazards;

> Integrate infrastructure security and resilience considerations, including the impacts of dependencies and cascading disruptions, into planning and investment decisions; and

> Recover quickly from disruptions to the normal functioning of community and regional infrastructure For the purpose of this document, “community” should be understood to include not just individual cities or towns, but also multijurisdictional regional authorities conducting planning and stakeholders with common interests or working on a common corridor to enhance the resilience of related infrastructure systems.

Planning for Resilient Infrastructure

The IRPF is not a definitive roadmap, but rather a flexible set of guidance documents and resources to kickstart infrastructure security and resilience planning and incorporate it into existing planning mechanisms.* While the IRPF is structured as a set of sequential steps, the user can choose which steps and sets of resources to more fully consider infrastructure in any existing or on-going planning process.

Communities can review the framework to determine where they are in the planning spectrum and choose the guidance and resources that best serve their needs.

Communities with limited time and resources may want to focus on the infrastructure sectors that support critical functions, such as energy, communications, transportation, and water and wastewater systems initially, with the potential to expand later.

Conversely, communities with more time and resources could consider all other critical infrastructure sectors deemed important and/or vital to the continued performance of key social and economic functions integral to the community or regional prosperity.

The IRPF helps users explore dependency relationships between infrastructure systems to better understand infrastructure risk, develop projects and strategies to address it, and identify funding and implementation resources to take action.

Ultimately infrastructure resilience contributes to a more resilient community, and can help develop and maintain a strong, safe, and economically vibrant place to live and work. This can help form a self-reinforcing cycle whereby increased social and economic resilience lead to increased infrastructure resilience and vice versa.

The Infrastructure Resilience Planning Framework (IRPF)

The IRPF is designed to be an easy-to-use framework for incorporating critical infrastructure resilience into local, regional, and Tribal plans. It is intended to help communities, regions, and infrastructure owners and operators better understand critical infrastructure risk, identify opportunities to enhance resilience, and inform policy and investment decisions.

Step 1, Lay the Foundation. Communities define and scope the planning effort, form a planning team to execute the effort, and review existing data, plans, studies, maps, and other resources.

Step 2, Critical Infrastructure Identification. Provides guidance to communities on how to identify and prioritize infrastructure and evaluate dependencies among infrastructure systems.

Step 3, Risk Assessment. Walks communities through the process of conducting a risk assessment of critical infrastructure to include evaluating vulnerabilities to threats and hazards, and consequences that may result.

Step 4, Develop Actions. Provides guidance on the development of a strategic action plan for addressing risk and enhancing infrastructure resilience by identifying and prioritizing potential solutions.

Step 5, Implement & Evaluate. Focuses on incorporating infrastructure resilience projects and strategies into community and regional plans and processes for measuring success.

To support these efforts, the IRPF also includes an assortment of resources to assist communities as they move through the various steps of the IRPF.

The IRPF encourages planners to take a functional, system-based approach when considering critical infrastructure. Individual infrastructure assets are only as important as the ultimate function they help provide:

it may not matter that a water treatment plant or pumping station is disrupted during an incident, for example, if there are adequate alternatives for providing potable water to the community until that system can be restored. Alternately, infrastructure systems are highly interconnected, and disruption in one may have cascading impacts that affect a range of other infrastructure systems. Because of these two factors, the IRPF encourages planners to consider the critical functions provided by infrastructure systems as well as the dependencies that exist within and between those systems. A strong understanding of these two factors can help planners identify strategies and projects to reduce their risk and make better investments in resilience.

The IRPF can be applied to all 16 sectors of critical infrastructure identified by Presidential Policy Directive 21 (PPD-21) – Critical Infrastructure Security and Resilience, which establishes a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure against physical and cyber threats. PPD-21 identifies 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, or any combination thereof. These critical infrastructure sectors are listed in Table 1, including a brief description of the typical components that comprise each sector. While PPD-21 takes a national perspective on critical infrastructure systems and assets, these sectors are also relevant at the local, state, and regional level and understanding risk to these systems can improve security, health and safety, and economic growth in your community.

Within every community and region, these sectors provide critical functions through infrastructure systems. These systems are composed of assets that are linked to and reliant on one another, and the continued operation of these systems is dependent not only on their own assets, but also other systems in other sectors. Importantly, nearly all sectors are reliant on energy, water and wastewater, communications, and transportation systems to function. The IRPF helps users examine these infrastructure systems, identify key dependencies within and between them, and incorporate that knowledge into planning.

Alignment to Planning Efforts and Federally Recognized Processes

It is important to note that the IRPF was developed to align with and inform other federal, state, local, tribal, and territorial planning efforts a community may be responsible for executing.

The steps and the associated resources can be easily integrated into other planning processes, such as comprehensive, hazard mitigation, environmental, capital improvement programming, and regional transportation. In fact, a key benefit of the IRPF is that it can help identify resilience projects that can be incorporated into these plans, allowing a community to build its resilience over the long-term and providing a prioritized list of potential projects that can be implemented with Federal funding following a disaster. Additionally, the IRPF aligns with and supports the Federal Emergency Management Agency (FEMA) National Mitigation Investment Strategy and the U.S. Government Accountability Office (GAO) Disaster Resilience Framework. While FEMA has established a series of “community lifelines” that, at first, may seem to be at odds with CISA’s sector-based approach, these two frameworks are in fact complementary. The community lifelines established by FEMA align with CISA’s infrastructure sectors and are intended to support response operations, whereas CISA’s 16 sectors can support steady-state activities.

In many ways, the IRPF complements and supplements other resilience guides and methodologies. For example, outputs from the IRPF can inform Step 3, Risk Assessment, and Characterizing the Built Environment of the National Institute of Standards and Technology (NIST) Community Resilience Planning Guide (CRPG). In addition, the infrastructure resilience assessment process documented in CISA’s Methodology for Assessing Regional Infrastructure Resilience closely aligns with the planning steps and guidance outlined in the IRPF.

Resources for Funding Opportunities and Technical Assistance

A key feature of planning is determining resource availability to develop and carry out planning and implementation. The IRPF provides a compendium of these resources in both a document and a user-friendly matrix, outlining funding opportunities and technical assistance that can help communities make planning a reality.

An Interview with Port of New Orleans

Ben Lane, CIPRNA event manager, met with Harbor Chief Police Melanie Montroll of the Port of New Orleans. She is a 21-year veteran of the force and serves as the department's first woman Chief of Police.

BL: I work for the team running Critical Infrastructure Protection & Resilience North America, the event happening in Baton Rouge, March 7-9, 2023. Really pleased to be talking with you today.

MM: Sounds good. And you.

BL: I gather you are the second generation to be working at the Port. Your father was there before you – is that correct?

MM: That is correct.

Melanie Montroll , Harbor Chief Police ,Port of New Orleans

BL: Lovely family line there.

MM: Yes, absolutely. Runs in the blood!

BL: Yes. Port NOLA is an important piece of infrastructure, obviously, within Louisiana. And it is a topic of conversation that will come up in the conference next year in March. Please explain broadly the work that you and your team do at the Port.

MM: Okay, so I am the Chief of

the Harbor Police Department. We are a full-fledged law enforcement agency that is responsible for keeping port tenants, workers, visitors safe when they visit the Port of New Orleans in our jurisdictions. So, we are a dedicated law enforcement, safety and security agency. We provide law enforcement services throughout the waterways within the port's three jurisdictions, which is Jefferson, Orleans and St. Bernard Parrish. Now, our mission is to contribute to the homeland defense by ensuring the safe, secure, efficient flow of cargo and cruise passengers for all the tenants and visitors that come through here.

BL: How do you view present emerging threats within your jurisdiction? What can you talk about in that area for us?

MM: So, as a critical infrastructure, the Port of New Orleans is working diligently to prevent cyber security risks, including identity-based cloud security threats, social engineering attacks or phishing, mobile security attacks, ransomware, and remote working. Our approach is we use a layered approach, solutions, to mitigate any potential threats. And obviously, on the law enforcement side, we work closely and directly with our IT department 24/7. That is continuous for us.

BL: Have you got a comment on the physical side? Any emerging threats that you can talk about on the physical side?

MM: Sure. On the physical side, obviously being a modern, multimodal gateway for global commerce and an in-demand cruise port, physical security is always going to be an issue for us, especially in terms of critical infrastructures. So, the physical threats we see, obviously are terrorist attacks. Obviously, drug smuggling, immigration. Those are all issues that we face as a Port, and our approach has always been to be proactive and to work with our federal partners, state partners, to ensure that we are keeping the Port and its tenants and visitors safe.

BL: I suppose that sort of does take us on a little bit more onto the protection side. So, we've talked about threats. What steps, broadly, are you using to protect yourself, protect the Port, protect your tenants and visitors? What are the steps you're taking there?

MM: First and foremost, our main step is actually being proactive instead of reactive. We are a proactive law enforcement agency. So, things that we do are visibility, proactive patrols, definitely collaborations with other federal partners. We work with the Coast Guard. We work with customs. We work with the FBI. We work with other law enforcement agencies that are in this area to make sure that we collaborate on threats that are not only facing the Port but facing the city and the state. So, it's definitely going to be a proactive approach, staying ahead of threats, staying up to date with current technologies. We were just awarded a FEMA grant here to upgrade the technology at the Harbor Police Department's Maritime Securities Operations Center, and that will give us the latest technology, allow us to keep the collaboration, and allow us to update cameras, barriers, fences, to make sure that we keep the Port safe.

BL: Can you give it a few words on the resilience side of your activities?

MM: It is imperative for our teams to use multiple overlapping solutions to build protection. This method ensures that if one system is compromised or fails, an overlapping system can catch the potential threat and mitigate it before it causes any real harm. And again, that ties into the investments in our infrastructure, the investments in technologies, and one good thing about the Port is we do have an IT team that's dedicated 24/7 to law enforcement to make sure that we can stay on top of being resilient and making sure that as times change, as threats change, we stay ahead of that.

BL: There's a cascading issue that we're talking about at the event, where one element of infrastructure, telecommunications for instance, drops out and causes an impact elsewhere. How do you view that in terms of the Port of New Orleans?

MM: The Port of New Orleans follows cybersecurity policies that are a key roadmap in responding to present issues. Our IT and HPD team have worked together to establish policies that not only protect employees but protect infrastructure and port tenants as we work to maintain a safe and secure, efficient, flow of the cargo and cruise passengers that come through here.

BL: That cascading effect on other big infrastructure within the state and beyond, do you have ideas around that and how that might be working for you?

MM: As I said, we are a very collaborative agency, so obviously what affects us affects other agencies, and vice versa. So yes, we are obviously diligently working to make sure that we stay in collaborative efforts with other agencies. But the key here is collaborating with those agencies, ensuring best practices. If they learn something new, they'll share it with us. We'll share with them. And we have a lot of teams, and we have a lot of exercises that we put on. We put on tabletops, but not only just the Port of New Orleans, but in the surrounding agencies, to make sure that we are all on one message.

BL: Okay, that brings us back to the point about being proactive.

MM: Absolutely. Absolutely. We are definitely proactive. Obviously, when the city was hit by ransomware a year ago, that was a big impact on everybody. So, it's not waiting for something to happen, it's being prepared for when and if it does happen so we can rebound from that.

BL: I'm so delighted always when I speak to people like you, people like you in that seat, and you're protecting us and you're doing the things that you need to do. We could talk for hours. Your history, the 21 years of service you've given, as well, is remarkable.

MM: It's a privilege and an honor for me to be in this position. It's definitely something I've dedicated my life to.

BL: Thank you for your time.

MM: Thank you.

See more at: https://portnola.com/info/news-media/press-releases/port-of-new-orleans-names-melanie-montroll-new-harbor-police-chief

Designing a flood early warning system (FEWS) for West Africa

The great West African drought that started in the 1970s was undoubtedly a turning point in the region's environmental discourse. It is well recognised as one of the most significant climate-driven disasters in recent history. The event was the onset of an era of rainfall uncertainty and variability, driving recurring floods and droughts across the region.

West Africa, an agglomeration of 16 countries, spans from the dense humid forests of the south to northern Saharan desertscapes (Figure.1). The region's rainfall cycle is controlled by the Intertropical Convergence Zone. Changes in rainfall patterns have been attributed to climate change as well as land-use changes. 'The Sahelian paradox', is the increase in river flows despite reducing rainfall seen in many river basins. The complexity of hydrological and regional wind systems make it difficult to accurately predict long-term rainfall trends and their consequences.

The Economic Community of West African States (ECOWAS) has invested significantly in drought management in the past. However, these nations have been unprepared for the sudden rise in floods over the last decade. In 2020, a year of particular flood severity, 198,000 homes were destroyed or damaged, 96,000 people were displaced and 2.2 million people were affected across West and Central Africa. If no action is taken, an estimated 32 million people will be forced to migrate internally by 2050.

In response to increasingly frequent disasters, many early warning systems for floods have been launched in West Africa. Flood early warning systems are typically designed around four broad considerations: knowledge of risks, monitoring and warning, response capacity and communication. These systems monitor real-time atmospheric conditions to predict weather conditions, and warn people and governments on how and when to act to minimise disaster impacts. Such tools are especially effective when emergency action plans are laid out and agreed upon by different stakeholders.

Existing flood early warning systems (FEWS) have not been able to meet stakeholders' needs regarding timeliness of information, geographical coverage, uninterrupted communication, accuracy and open ownership. To increase the adoption, effectiveness and usefulness of warning systems, stakeholder engagement in the design phase is crucial. Generally, empirical evidence on the effectiveness of participatory processes in sustainability science and disaster planning has been weak.

The EU Horizon 2020 FANFAR (Reinforced cooperation to provide operational flood forecasting and alerts in West Africa) project aimed to change this. Within FANFAR's broader aim of developing a FEWS, our research focused on designing such a system in collaboration with 50-60 stakeholders from 17 countries. Stakeholders included emergency managers, representatives from regional and national hydrological services and river basin institutions. Two key participating organisations were the West African consortium members AGRHYMET Regional Center and the Nigeria Hydrological Services Agency.

INTERPOL maritime operation nets terrorist suspects

Two terrorist suspects wanted internationally under Red Notices have been arrested during an international maritime border operation coordinated by INTERPOL.

Another eight investigative leads linked to terrorism were generated during Operation Neptune IV (1 July – 3 September) which targeted terrorist suspects and other criminals involved in serious organized crime travelling via maritime routes between North Africa and Southern Europe.

The intelligence-led operation was supported by an INTERPOL team on the ground, and also targeted criminal networks involved in the drugs trade, firearms trafficking, human trafficking and people smuggling.

Officials at seaports and airports in eight countries – Algeria, Cyprus, France, Italy, Lebanon, Morocco, Spain and Tunisia – carried out more than 2.6 million checks across INTERPOL's databases for stolen and lost travel documents, nominal data and stolen vehicles via its I-24/7 secure global police communications network.

These checks generated 140 hits, resulting in 14 additional arrests following seizures worth USD 3.6 million, including: 33 kg of cocaine, some 39,400 ecstasy pills, 133 kg of cannabis, and ten stolen cars. Ten firearms were also seized.

The operation also targeted illicit migrant flows, with authorities in France, Italy and Spain arresting suspected human traffickers and people smugglers and intercepting 13 irregular migrants.

With thousands of vehicles and passengers crossing international borders via maritime routes every year, INTERPOL Secretary General Jürgen Stock said that cross-border initiatives such as Neptune demonstrate how concerted law enforcement action can disrupt terrorist threats and criminals on the move.

Operation across Africa identifies cyber-criminals and at-risk online infrastructure

Law enforcement officials from 27 INTERPOL countries joined forces in the Africa Cyber Surge Operation to counter cybercrime across the continent.

Against the backdrop of the huge financial losses suffered by companies, businesses and individuals, the four-month operation (July to November 2022) saw officers detect, investigate and disrupt cybercrime through coordinated law enforcement activities utilizing INTERPOL platforms, tools and channels, in close cooperation with AFRIPOL.

Operational results

Coordinated from an INTERPOL Command Centre in Kigali, Rwanda, the operation focused on removing the enablers of cybercrime.

Actionable intelligence

Investigations were shaped by intelligence provided by INTERPOL's private sector partners including British Telecom, Cyber Defense Institute, Fortinet's FortiGuard Labs, Group-IB, Kaspersky, Unit 42-Palo Alto Networks, Shadowserver and Trend Micro.

The information also contributed to the development of 28 INTERPOL Cyber Activity Reports that highlighted the various threats and types of criminal activity and outlined the recommended actions to be taken by national authorities.

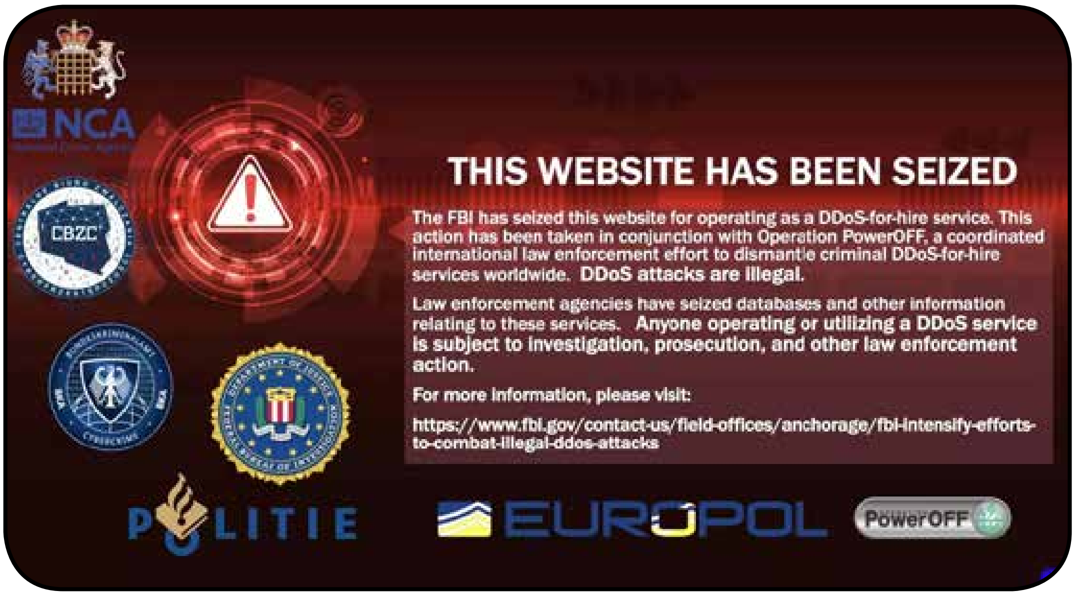
Participating investigators worked in their home countries in collaboration with National Cyber Emergency Response Teams, Internet Service Providers and Hosting Providers who were notified of the potential vulnerability in their network infrastructure within their jurisdictions.

This collaboration proved very successful with 80% of identified ISPs engaging with law enforcement to mitigate the risks, identify weaknesses in their infrastructure and notify customers.

Of the participating countries, 18 have recognized Cyber Emergency Response Teams (CERTs), all of whom are actively working with law enforcement agencies and ISPs. Agreements have been set up between these organizations to formalize future responses.

INTERPOL

Global crackdown against DDoS services shuts down most popular platforms



THIS WEBSITE HAS BEEN SEIZED

The FBI has seized this website for operating as a DDoS-for-hire service. This action has been taken in conjunction with Operation PowerOFF, a coordinated international law enforcement effort to dismantle criminal DDoS-for-hire services worldwide. **DDoS attacks are illegal.**

Law enforcement agencies have seized databases and other information relating to these services. **Anyone operating or utilizing a DDoS service is subject to investigation, prosecution, and other law enforcement action.**

For more information, please visit:

https://www.fbi.gov/contact-us/field-offices/anchorage/fbi-intensify-efforts-to-combat-illegal-ddos-attacks

Some fifty of the world's biggest booter services, designed to enable users to launch crippling distributed denial-of-service (DDoS) against critical online infrastructure, have been taken down as part of an international crackdown against DDoS service providers.

Known as Operation Power Off, this operation saw law enforcement in the United States, the United Kingdom, the Netherlands, Poland and Germany take action against these types of attacks which can paralyse the internet.

The services seized were by far the most popular DDoS booter services on the market, receiving top billing on search engines. One such service taken down had been used to carry out over 30 million attacks.

As part of this action, seven administrators have been arrested so far in the United States and the United Kingdom, with further actions planned against the users of these illegal services.

International police cooperation was central to the success of this operation as the administrators, users, critical infrastructure and victims were scattered across the world. Europol's European Cybercrime Centre coordinated the activities in Europe through its Joint Cybercrime Action Taskforce (J-CAT).

This international sweep follows previous editions of Operation Power Off which targeted the administrators and users of the DDoS marketplace webstresser.org.

Participating authorities

- United States: US Department of Justice (US DOJ), Federal Bureau of Investigation (FBI)
- United Kingdom: National Crime Agency (NCA)
- The Netherlands: National High Tech Crime Unit Landelijke Eenheid, Cybercrime team Midden-Nederland, Cybercrime team Noord-Holland and Cybercrime team Den Haag
- Germany: Federal Criminal Police Office (Bundeskriminalamt), Hanover Police Department (Polizeidirektion Hannover), Public Prosecutor's Office Verden (Staatsanwaltschaft Verden)
- Poland: National Police Cybercrime Bureau (Biuro do Walki z Cyber-przestčpczočcič)

DDoS-ing is a crime

DDoS booter services have effectively lowered the entry barrier into cybercrime: for a fee as low as EUR 10, any low-skilled individual can launch DDoS attacks with the click of a button, knocking offline whole websites and networks by barraging them with traffic.

The damage they can do to victims can be considerable, crippling businesses financially and depriving people of essential services offered by banks, government institutions and police forces.

Emboldened by a perceived anonymity, many young IT enthusiasts get involved in this seemingly low-level crime, unaware of the consequences that such online activities can carry.

DDoS-ing is taken seriously by law enforcement. Size does not matter – all levels of users are on the radar of law enforcement, be it a gamer booting out the competition out of a video game, or a high-level hacker carrying out DDoS attacks against commercial targets for financial gain.

The side effects that a criminal investigation could have on the lives of these DDoS users can be serious, going as far as a prison sentence in some countries.

critical infrastructure PROTECTION AND RESILIENCE AMERICAS

March 7th-9th, 2023

BATON ROUGE, LOUISIANA

A Homeland Security Event

Collaborating and Cooperating for Greater Security

For Securing Critical Infrastructure and Safer Cities

Co-Hosted & Supported by::

International Association of CIP Professionals

INFRAGARD MEMBERS ALLIANCE LOUISIANA

REGISTER TODAY
Early Bird Discount
deadline
February 7th,2023

SPECIAL RATES FOR GOVERNMENT AND OWNER/OPERATORS
Register by February 7th
see inside for details

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

Preliminary Conference Programme

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

Register online at www.ciprna-expo.com

Leading the debate for securing America's critical infrastructure

Supporting Organisations:

International Association of CIP Professionals

INFRAGARD MEMBERS ALLIANCE LOUISIANA

IACI

ISIO

HS&RC

S T I M E

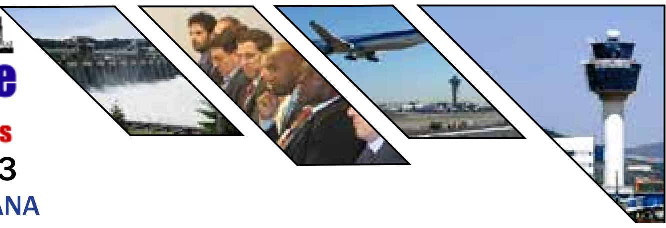
Media Partners:

World Security-index.com

critical infrastructure PROTECTION AND RESILIENCE NEWS

critical infrastructure
PROTECTION AND RESILIENCE AMERICAS

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



A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Welcome to the 4th Critical Infrastructure Protection and Resilience North America

There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety.

Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure. This directive supersedes Homeland Security Presidential Directive 7.

We must be prepared!

The Nation's critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure – including assets, networks, and systems – that are vital to public confidence and the Nation's safety, prosperity, and well-being.

Critical infrastructure must be secure and able to withstand and rapidly recover from all hazards. Achieving this will require integration with the national preparedness system across prevention, protection, mitigation, response, and recovery.

This directive establishes national policy on critical infrastructure security and resilience. This endeavor is a shared responsibility among the Federal, state, local, tribal, and territorial (SLTT) entities, and public and private owners and operators of critical infrastructure (herein referred to as "critical infrastructure owners and operators"). This directive also refines and clarifies the critical infrastructure-related functions, roles, and responsibilities across the Federal Government, as well as enhances overall coordination and collaboration. The Federal Government also has a responsibility to strengthen the security and resilience of its own critical infrastructure, for the continuity of national essential functions, and to organize itself to partner effectively with and add value to the security and resilience efforts of critical infrastructure owners and operators.

Critical Infrastructure Protection and Resilience North America will bring together leading stakeholders from industry, operators, agencies and governments to collaborate on securing North America.

The conference will look at developing on the theme of previous events in helping to create better understanding of the issues and the threats, to help facilitate the work to develop frameworks, good risk management, strategic planning and implementation.

Why the Need for Such a Discussion?

All Federal department and agency heads are responsible for the identification, prioritization, assessment, remediation, and security of their respective internal critical infrastructure that supports primary mission essential functions. Such infrastructure needs to be addressed in the plans and executed to the requirements of the National Continuity Policy.

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

This guide, correct at the time of printing, aims to provide you with the information you need to plan your attendance to this key conference, including the latest conference programme, speaker line up and schedule of events.

We have special rates for government and operators of critical national infrastructure, so please look fr these deals in this guide.

Please register online at www.ciprna-expo.com.

We look forward to welcoming you to Critical Infrastructure Protection & Resilience North America and the L'Auberge Hotel & Casino, Baton Rouge on March 7th-9th, 2023.

Welcome from the Conference Chairman

Dear Friends and Colleagues,

Collaborating and Cooperating for Greater Security

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

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

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

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

Unfortunately, we all have to understand that the days of simple security measures are long gone, the dynamics have changed considerably and so to must our total approach to security and resilience. There is, therefore, a continual need to review, develop and update policies, practices, procedures and technologies to meet those growing and changing demands.

In seeking to address these issues we have an exciting agenda lined up with some excellent speakers covering a wide range of important topics, presenting their thoughts on the way forward and their views on the current and emerging good practice that is in place across the world.

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

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

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

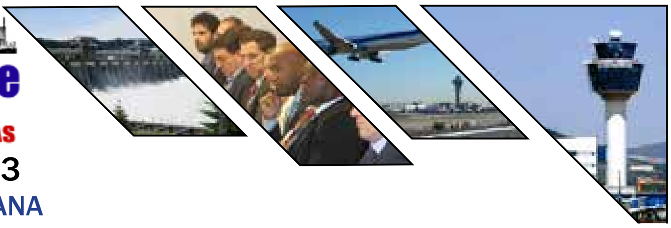
The exhibition taking place alongside the conference will be showcasing some of the latest technologies that are currently being utilised internationally within both the physical and cybersecurity environments across a range of infrastructure sectors.

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

John Donlon QPM FSyl
Conference Chairman

critical infrastructure
PROTECTION AND RESILIENCE AMERICAS

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



A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Exhibition Opening Hours

Tuesday March 7th	1.00pm to 7.30pm
Wednesday March 8th	9.30am to 5.30pm
Thursday March 9th	9.30am to 4.30pm

On-Site Registration Hours

Tuesday March 7th	8.00am to 6.00pm
Wednesday March 8th	8.30am to 5.00pm
Thursday March 9th	8.30am to 4.00pm

REGISTER ONLINE AT WWW.CIPRNA-EXPO.COM

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

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 infratructure owner/operators.

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

EARLY BIRD DISCOUNT - deadline February 7th, 2023

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

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

Discounts for Members of Supporting Associations

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

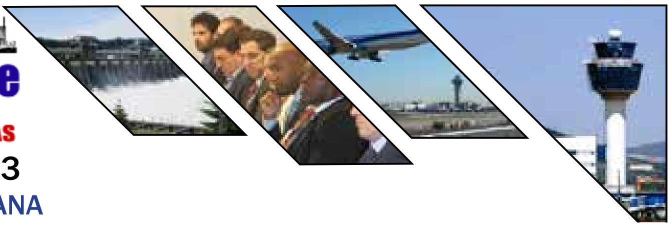
- INFRAGARD LA
- The International Emergency Management Society (TIEMS)
- National Security & Resilience Consortium (NS&RC)
- International Association of CIP Professionals (IACIPP)
- International Security Industry Organization (ISIO)
- International Association of Certified ISAOs (IACI)
- Security Partners Forum (SPF)
- Global Institute for CyberSecurity & Research (GICSR)

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

critical infrastructure
PROTECTION AND RESILIENCE AMERICAS

March 7th-9th, 2023

BATON ROUGE, LOUISIANA



A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Schedule of Events

Tuesday March 7th, 2023

1:00pm - Exhibition Opens

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

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

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

5:30pm - Networking Reception in Exhibition Hall

Wednesday March 8th, 2023

Track One

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

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

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

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

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

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

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

Track Two

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

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

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

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

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

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

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

Thursday March 9th, 2023

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

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

11:15am - 12:30pm - Session 7a: Access to Funding for CI Security

9:00am-10:30am - Session 6b: Developing Resilience Strategies

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

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

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

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

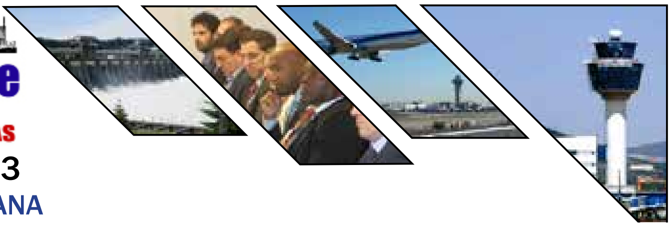
3:30pm-4:00pm - Review, Discussion and Conference Close

4.30pm - Expo Close

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

critical infrastructure
PROTECTION AND RESILIENCE AMERICAS

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



A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Tuesday March 7th, 2023

Workshops Room

11:00am-1:00pm - Workshop: Establishing a CIPR Community

Wednesday March 8th, 2023

Workshops Room

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

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

11:15am - 12:30pm - Session 3c: The International Emergency Management Society Workshop

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

2:00pm-3:30pm - Session 4c: CT Briefing by HS Today

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

4:15pm - 5:30pm - Session 5c: CT Briefing by HS Today

Thursday March 9th, 2023

9:00am-10:30am - Session 6c: TBC

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

11:15am - 12:30pm - Session 7c: TBC

Who Should Attend

Critical Infrastructure Protection and Resilience North America is for:

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

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

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

Exhibitor Showcasing in the Expo:

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

AXIS® COMMUNICATIONS

CAPITOL Technology University

IACI INTERNATIONAL ASSOCIATION OF CERTIFIED ISAOS

U.S. DEPARTMENT OF HOMELAND SECURITY CISA CYBER+INFRASTRUCTURE

International Association of CIP Professionals

CMA Technology Solutions

Johnson Controls

Genetec™

U.S. DEPARTMENT OF HOMELAND SECURITY Homeland Security

HEXAGON

ECHODYNE

critical infrastructure PROTECTION AND RESILIENCE NEWS

TEXAS A&M ENGINEERING TEEX EXTENSION SERVICE

LVT

INFRAGARD MEMBERS ALLIANCE LOUISIANA

LITEYE. Beyond Human Vision.

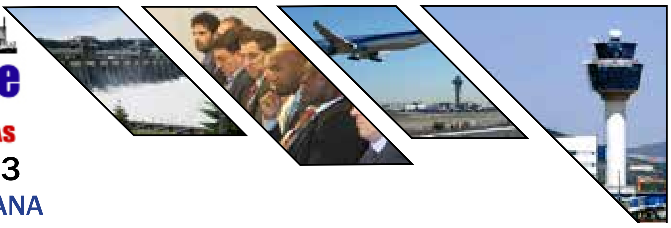
GTSC Government Technology & Services Coalition's HOMELAND SECURITY TODAY.US

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

critical infrastructure
PROTECTION AND RESILIENCE AMERICAS

March 7th-9th, 2023

BATON ROUGE, LOUISIANA



A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Tuesday March 7th

Conference Programme

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

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

Dr David Mussington, Assistant Director for the Infrastructure Security Division, CISA, US Department of Homeland Security (DHS)

Senior Representative, Federal Emergency Management Agency (FEMA)*

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

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

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

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

Chair: John Donlon QPM, FSI

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

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

PPPs and Communities - Lester Millet, President, Infragard LA

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

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

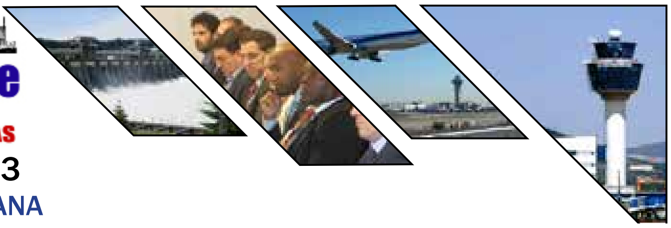
5:30pm-7:30pm - Networking Reception in Exhibit Hall

*invited

critical infrastructure
PROTECTION AND RESILIENCE AMERICAS

March 7th-9th, 2023

BATON ROUGE, LOUISIANA



A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Wednesday March 8th

Track One

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

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

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

Vanessa Tibbits, Associate Special Agent in Charge, FBI

Steve Zeringue, WMD Co-ordinator, FBI*

Emerging Cyber Threats - Senior Representative, NSA*

Senior Representative, NCTC*

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

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

The energy sector has become the most critical of sectors. Without power, driven by oil, gas and renewable energies, all other CI stops. Recent cyber attacks on the energy sector, as well as natural hazards, from hurricanes in the Gulf to fires in California, gives much room for thought on how we best protect our most vital assets, including IT/OT and SCADA systems. How can we mitigate the impact of an attack or outage on the wider community and society.

Amanda Rogers, Fire, Safety & Security Representative, LOOP*

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

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

Darin Dillon, Senior Director Energy, LenelS2

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

Track Two

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

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

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

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

George Markowsky, The International Emergency Management Society

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

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

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

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

Ronald Pavlik, Deputy Assistant Administrator, Transport Security Administration

Senior Representative, New Orleans International Airport*

Rail Operator TBC

Senior Representative, Port of South Louisiana*

J. Eric Boyette, Secretary of Transport, North Carolina Department of Transportation*

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

Wednesday March 8th

Track One

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

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

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

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

Joshua Tannehill, Sr. Manager, Lumen Trust & Safety

Mike Regan, VP Business Performance, Telecommunications Industry Association (TIA)

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

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

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

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

Logistics Company TBC

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

TBC

Track Two

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

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

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

Joint Collaboration to Enhance Chemical Security - Kelly Murray, Associate Director for Chemical Security, CISA

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

TBC

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

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

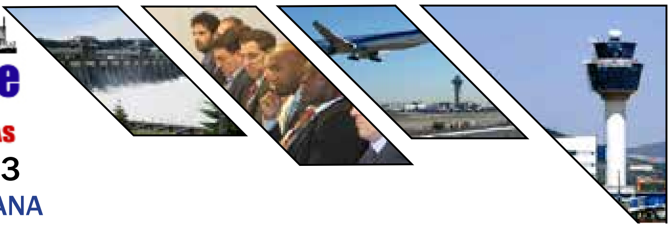
As we rely more and more heavily on satellites for communications, navigation, observation and security/defence, the requirement to ensure that space based systems are both secure and resilient becomes more urgent. Government networks and systems need to lead security and resilience across agencies and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

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

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

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

Senior Representative, NASA*



Thursday March 9th

Track One

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

Being prepared for the changing threat environment can benefit greatly in mitigating its impact on infrastructure and the broader community, ensuring resilience, safety and security. How can we counter these emerging physical and cyber threats to minimise loss of service and financial impact?

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

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

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

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

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

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

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

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

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

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

TBC

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

Track Two

9:00am-10:30am - Session 6b: Funding for CI Preparedness and Resilience Planning

With the formation of the National Infrastructure Bank, whose responsibility it is to fund community CI planning and preparedness, what does the funding cover and how can communities access this funding?

Jeff Gaynor, President, National Resilience

Minna LeVine, CEO/President, SMART Community Exchange

TBC

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

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

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

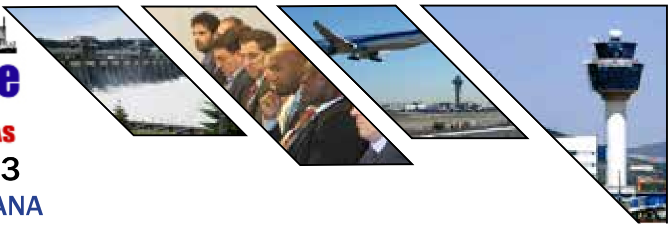
Secure Tomorrow Series: A Strategic Foresight Toolkit to Prepare for the Future - Leigh J. Blackburn, Ph.D., Senior IT Specialist, Program Manager for Secure Tomorrow Series, CISA

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

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

TBC

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



Thursday March 9th

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

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

Moderator: John Donlon QPM FSI

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

Randy Meshell, Federal Preparedness Coordinator Region VI, FEMA

Jeff McKee, Regional Coordinator, CISA

Lester Millet, President, Infragard LA

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

Jeff Gaynor, President, National Resilience

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

Networking Reception

Tuesday March 7th
5.30pm - 7:30pm
Exhibition Floor

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

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

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

We look forward to welcoming you.

The Venue and Accommodation

L'Auberge Hotel & Casino
777 L'Auberge Ave
Baton Rouge 70820
Louisiana

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

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

Baton Rouge L'Auberge has a refreshing rooftop swimming pool with poolside cabanas and a full bar with views of the Mississippi River. A fitness centre is available for relaxation. Self-parking is available to hotel guests at no extra charge. Valet parking is also offered.

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

Accommodation

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

Book your hotel accommodation at the **L'Auberge Hotel & Casino** at www.ciprna-expo.com/hotel-booking

Delegates/attendees can make reservations in the following way:

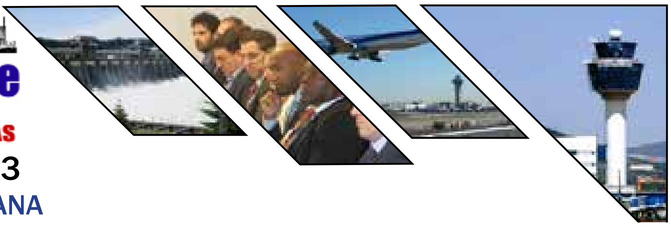
- Online: Reservations can be made online at www.ciprna-expo.com/hotel-booking

We look forward to welcoming you to Baton Rouge.

critical infrastructure
PROTECTION AND RESILIENCE AMERICAS

March 7th-9th, 2023

BATON ROUGE, LOUISIANA



A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Why participate and be involved?

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

Your participation will gain access to this key target audience:

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

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

www.ciprna-expo.com

How to Exhibit

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

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

Ray Beauchamp
Americas
E: rayb@torchmarketing.co.uk
T: +1 559-319-0330

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

Sam Most
Mainland Europe & Turkey
E: samm@torchmarketing.co.uk
T: +44 (0) 208 123 7909

Sponsorship Opportunities

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

Some of the sponsorship package opportunities are highlighted here.

- Platinum Sponsor - $12,500
- Gold Sponsor - $8,950
- SIlver Sponsor - $6,950
- Bronze Sponsor - $4,950
- Conference Proceedings Sponsor - $3,950
- Delegate Folder Sponsor - $3,950
- Networking Reception Sponsor - $2,950
- Coffee Break Sponsor - $2,950
- Lanyard Sponsor - $2,950
- Badge Sponsor - $2,950

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

Please enquire for further details.

Exhibiting Investment

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

Table Top Exhibit 5’x7’ - $2,500
Table Top Exhibit 10’x10’ - $4,500
Raw space with 1 x table and 2 x chairs, pipe and drape, electrical socket, wi-fi, 1 Exhibitor Delegate pass with full conference access, lunch and coffee breaks included, listing in the official event guide and website.

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

ASK ABOUT OUR BOOKING BUNDLES FOR EXTRA EXPOSURE

ALL PRICES SUBJECT TO 9.95% LOUISIANA/BATON ROUGE SALES TAX

critical infrastructure PROTECTION AND RESILIENCE AMERICAS

March 7th-9th, 2023

BATON ROUGE, LOUISIANA

A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Sponsors and Supporters:

We wish to thank the following organisations for their support and contribution to Critical Infrastructure Protection & Resilience North America 2023.

Supported & Co-Hosted by:

International Association of CIP Professionals

INFRAGARD MEMBERS ALLIANCE LOUISIANA

Silver Sponsors:

Johnson Controls

Bronze Sponsors:

TEXAS A&M ENGINEERING TEEX EXTENSION SERVICE

Genetec

ECHODYNE

Flagship Media Partners:

critical infrastructure PROTECTION AND RESILIENCE NEWS

GTSC HOMELAND SECURITY TODAY.US

Coffee Break Sponsor:

AXIS COMMUNICATIONS

Supporting Organisations:

SMARTX Community Exchange

IACI INTERNATIONAL ASSOCIATION OF CERTIFIED ISAOs

T S I M E

ISIO - International Security Industry Organization

SPF SECURITY PARTNERS' FORUM

NS&RC

Media Supporters:

BORDER SECURITY REPORT

govCIO OUTLOOK

TSI TRANSPORT SECURITY INTERNATIONAL www.tsi-mag.com

World Security-index.com

Owned & Organised by:

TORCH

World Border Security Congress

25TH-27TH APRIL 2023

SKOPJE, NORTH MACEDONIA (BALKANS)

www.world-border-congress.com

Developing Border Strategies Through Co-operation and Technology

Co-Hosted and Supported by:

РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА ПОЛИЦИЈА POLICE

INVITATION TO ATTEND - REGISTER ONLINE TODAY

You are invited to attend the 2023 World Border Security Congress

The Republic of North Macedonia is a landlocked country in the Southeastern region of Europe known as the Balkans. It gained independence in 1991 as one of the successor states of Yugoslavia.

In March 2020, North Macedonia acceded to NATO, becoming the 30th member state and accession process to join the European Union remains ongoing.

Ranked as the fourth "best reformatory state" out of 178 countries ranked by the World Bank in 2009, North Macedonia has undergone considerable economic reform since independence. North Macedonia has witnessed steady, though slow, economic growth and has implemented policies focused on attracting foreign investment and promoting the development of small and medium-sized enterprises (SMEs).

By virtue of its position North Macedonia sits on the Balkan route for illegal migration into the European Union and therefore faces border challenges that require a collective, collaborative, and holistic response, making it the ideal place for the next meeting of the 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 Skopje, North Macedonia on 27th-29th April 2023 for the next gathering of border and migration management professionals.

www.world-border-congress.com

for the international border management and security industry

Supported by:

OSCE Organization for Security and Co-operation in Europe
European Association of Airport and Seaport Police
AFRICAN UNION
MARRI Migration, Asylum, Refugees Regional Initiative
ISIO
International Association of CIP Professionals
NS&RC

Media Partners:

World Border Security Network
BORDER SECURITY REPORT
World Security-index.com