critical infrastructure PROTECTION AND RESILIENCE NEWS

Official Magazine of

International Association of CIP Professionals

WINTER 2025/26
www.cip-association.org

FEATURE:
Beyond Compliance: Conceptual and Implementation Cycles in Critical Infrastructure Protection

FEATURE:
CIP-014-4 Is Expanding the Physical Security Perimeter: What Municipally Owned Utilities Must Prepare for Now

FEATURE:
From Situational Awareness to Operational Advantage: The Evolving Role of Live Video in Critical Infrastructure Protection

LESSONS FROM UKRAINE: WHAT CRITICAL INFRASTRUCTURE PROTECTION PROFESSIONALS SHOULD LEARN ABOUT INFORMATION WARFARE

Critical Infrastructure Protection Week *in Europe*

20th–22nd October 2026 – Brussels, Belgium

International Association of CIP Professionals

critical infrastructure PROTECTION AND RESILIENCE EUROPE

SAVE THE DATES

Building Resilience for the Critical Connected World

The International Association for CIP Professionals is delighted to be hosting the next CIP Week in Europe in Brussels, Belgium for the next annual industry gathering in October 2026.

Critical Infrastructure Protection and Resilience Europe (CIPRE is Europe's go-to event for critical infrastructure protection and resilience — bringing together top minds from industry, government, and beyond to shape the future of security and resilience across vital sectors.

CALL FOR PAPERS - Deadline 31st March 2026

The CIPRE Conference Committee are currently accepting abstracts for consideration for inclusion in the 2026 conference agenda.

Visit www.cipre-expo.com for more details how you can be a speaker or benefit from being a sponsor at the event.

Join us in Brussels for the third CIP Week in Europe and the 11th Critical Infrastructure Protection and Resilience Europe discussion on securing Europe's critical infrastructure.

www.cipre-expo.com

Leading the debate for securing Europe's critical infrastructure

Co-Hosted by:

International Association of CIP Professionals

Media Partners:

critical infrastructure PROTECTION AND RESILIENCE NEWS

To discuss sponsorship opportunities contact:

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

Bruce Bassin
(Americas)
E: bruceb@torchmarketing.co.uk
T: +1-702.600.4651

GETTING PREPARED FOR 2026 AND WHAT THE YEAR MAY HOLD

As we begin a new year, we hope that more steady times may lay ahead - back to some sort of normality and knowing what to expect to be able to better plan and prepare. Unfortunately, it seems that 2026 has started off with just as much uncertainty as it did a year ago.

The threat of war appears to loom closer with tensions rising in the Middle East and now parts of Central/South America, on top of Ukraine, the threats from China, North Korean and other unfriendly nation states (and indeed some friendly allies!).

Attacks and additional threats against critical infrastructure are greater than ever in such uncertain times, and the consequences of disruption now reach far beyond any single organisation, sector, or border.

Energy, water, transport, communications, healthcare, and financial systems are increasingly interconnected. A weakness in one area can quickly cascade into many others, affecting daily life, economic stability, and public trust.
At the same time, digital transformation continues at pace. Cloud services, automation, and artificial intelligence bring huge opportunity, but they also expand the attack surface and introduce new dependencies that must be understood and managed.

Yet, despite this challenging backdrop, there are also reasons for cautious optimism. Awareness of risk has never been higher. Boards and senior leaders are more engaged in resilience, security, and continuity planning than ever before. Collaboration between government, industry, and international partners continues to improve, driven by a shared recognition that no organisation can stand alone against today's threats. This magazine exists to support that collective effort.

In this edition, we explore the evolving risk landscape and look at practical steps organisations can take to strengthen resilience, both physical and digital. You will find insights from practitioners working on the front line, analysis of emerging trends, and lessons learned from recent incidents.

As we move further into 2026, uncertainty may remain a constant. How we respond to it is not. By staying informed, connected, and proactive, we can navigate these turbulent times with greater confidence and clarity. This can begin at the next gathering of the industry at Critical Infrastructure Protection & Resilience North America in Baton Rouge, LA on March 10th-12th - more details can be seen inside.

Thank you for reading, and for the vital work you do in helping to protect the systems and services we all rely on.

Thank you.

Ed.

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.

Lessons from Ukraine: What Critical Infrastructure Protection Professionals Should Learn About Information Warfare

By Natasia Kalajdziovski, PhD, Senior Fusion Threat Intelligence Analyst, SecAlliance

Information Warfare Is Infrastructure Warfare

Critical infrastructure protection has traditionally focused on tangible risks: physical sabotage, natural hazards, equipment failure and, more recently, cyberattacks and protest action. These threats remain central. However, the war in Ukraine has revealed a parallel reality that can no longer be treated as secondary. Information warfare – particularly disinformation – has become a core component of infrastructure targeting.

In Ukraine, attacks on energy, transportation, water, and communications systems were rarely isolated technical events. They were embedded within broader influence campaigns designed to shape how populations, governments, and international audiences perceive those events.

Disinformation did not simply accompany infrastructure attacks: it prepared the ground for them, magnified their effects, and

prolonged their impact.

The integration of physical, cyber, and influence operations represents a shift in how critical infrastructure is contested. It challenges existing protection and resilience models, which often assume that technical restoration equates to recovery. Ukraine's experience shows that even when systems are repaired, trust, confidence and social cohesion may remain damaged – sometimes irreversibly.

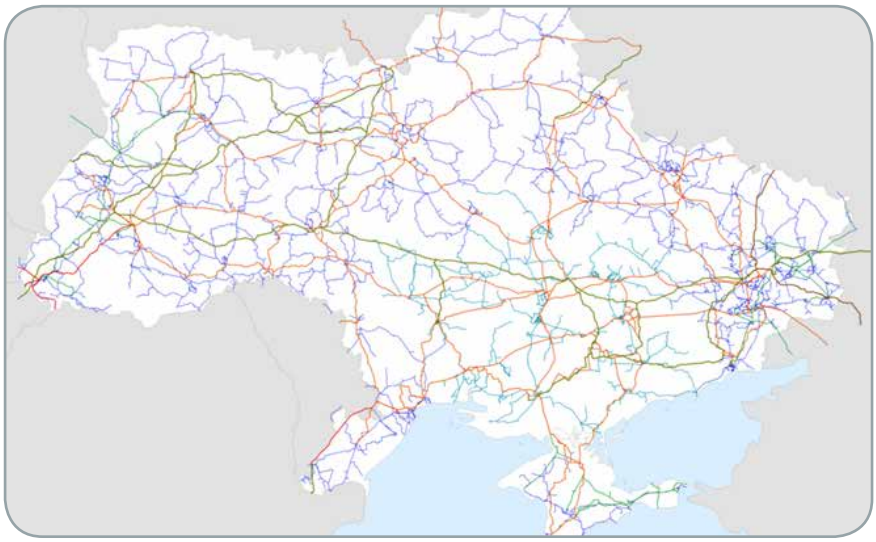
The lessons from Ukraine are not limited to armed conflict. The same techniques are increasingly applied during peacetime crises, natural disasters, industrial accidents, and political instability. For critical infrastructure professionals globally, understanding information warfare is now a prerequisite for resilience.

Disinformation as a Preparatory Tool

One of the clearest patterns observed in Ukraine was the use of disinformation well before infrastructure attacks occurred. Russian-aligned media outlets, social media networks, and proxy voices consistently promoted narratives portraying Ukrainian infrastructure as outdated, fragile, corruptly managed, or on the brink of collapse.

These narratives served several strategic purposes:

First, they normalised failure. By repeatedly asserting that infrastructure collapse was inevitable, disinformation lowered public expectations and reduced the perceived shock value of outages. When attacks occurred, they appeared to confirm preexisting beliefs rather than signal deliberate aggression.



Second, these narratives undermined institutional credibility. Infrastructure operators, regulators, and government officials were framed as incompetent or dishonest. This eroded trust before any incident took place, ensuring that official communications would be met with scepticism during crises.

Third, preparatory disinformation shaped attribution. When outages occurred, audiences were already primed to blame mismanagement or systemic decay rather than external attack. This confusion benefited the attacker by obscuring responsibility and complicating international response.

For infrastructure protection professionals, this highlights an often-overlooked warning sign: persistent, coordinated narratives questioning infrastructure reliability may indicate more than public dissatisfaction. They can be early indicators of hostile influence activity aligned with future disruption.

Exploiting the Moment of Crisis

The second phase of information warfare unfolded during active infrastructure disruptions. In Ukraine, disinformation campaigns were activated almost immediately following missile strikes, cyber incidents, or sabotage.

Within minutes, false or misleading claims appeared across multiple platforms, often repeating similar themes:

- Exaggerated estimates of outage scale and duration
- False causes, including fabricated internal failures or accidents
- Claims that authorities were concealing the truth
- Warnings of secondary threats, such as water contamination or fuel shortages

These narratives exploited a universal vulnerability: the information vacuum that emerges during fast-moving incidents. In the early stages of any infrastructure failure, details are incomplete, assessments are ongoing, and officials may hesitate to communicate prematurely. Disinformation thrives in this uncertainty.

In Ukraine, hostile narratives often outpaced official messaging, becoming the first version of events many people encountered. Once established, these narratives proved difficult to dislodge, even

Overhead electrical transmission line in Ukraine — representative of the energy grid that has been a frequent focus of both kinetic attacks and related disinformation. Source: Wikimedia Commons, CC BY-SA 4.0.

after accurate information became available.

The result was not merely confusion, but operational impact. Emergency services faced increased pressure due to panic-driven behaviour. Infrastructure staff were targeted by public anger fuelled by false accusations. Compliance with emergency guidance declined as trust eroded.

This pattern is not unique to Ukraine. Any infrastructure incident – whether caused by natural disaster, accident, or attack – creates similar informational vulnerabilities. The difference lies in whether adversaries are prepared to exploit them.

The Post-Incident Information Battle

Infrastructure protection often defines success as restoration of service. Ukraine's experience demonstrates that this definition is incomplete. Information warfare continued long after power was restored, trains resumed operation, or communications networks stabilised.

Post-incident disinformation campaigns focused on delegitimising recovery efforts. Common narratives included claims that repairs were superficial, that reported restoration was fabricated, or that funds allocated for recovery were being stolen. In some cases, restored services were portrayed as unsafe or intentionally compromised.

These narratives had cumulative effects. Over time, they fostered a sense of permanent vulnerability and institutional failure. Each subsequent incident, even minor ones, triggered outsized reactions because public confidence had already been degraded.

For societies dependent on complex infrastructure systems, this erosion of trust poses a strategic risk. Public cooperation is essential during outages, conservation measures, evacuations, and recovery efforts. When trust collapses, resilience collapses with it.

Energy Infrastructure: Visibility and Vulnerability

Energy infrastructure emerged as a primary target of integrated attacks in Ukraine, both because of its strategic importance and its visibility. Power outages are immediately felt across society, making them ideal opportunities for influence operations.

Russian disinformation consistently framed energy disruptions as evidence of state failure. At the domestic level, narratives emphasised government incompetence and inevitability of collapse. Internationally, messaging warned that Ukrainian instability threatened regional energy security, aiming to undermine external support.

The combination of physical damage and narrative exploitation transformed grid attacks into broader political and psychological events. Even limited outages were portrayed as existential crises.

Globally, energy infrastructure shares these characteristics. It is highly visible, politically sensitive, and closely tied to public confidence. Whether the cause is hostile action, extreme weather, or technical failure, energy disruptions offer fertile ground for disinformation.

Resilience strategies that focus solely on redundancy and hardening overlook this reality. Narrative management – ensuring credible, timely, and transparent communication – is a critical defensive capability for the energy sector.

Transportation and Logistics: Perception Versus Reality

Transportation and logistics infrastructure played a subtler but equally important role in Ukraine's information war. Disruptions to rail networks, ports, and supply chains

were frequently exaggerated through disinformation to suggest nationwide paralysis.

In practice, many of these disruptions were localised or temporary. However, narratives portraying systemic collapse created disproportionate psychological impact. They undermined confidence in the state's ability to function and fuelled perceptions of chaos.

This illustrates a key insight: the strategic value of infrastructure disruption lies not only in material impact, but in perceived impact. Disinformation can amplify limited damage into a crisis of legitimacy.

Transportation systems worldwide share similar vulnerabilities. They are complex, interdependent, and largely invisible until something goes wrong. When disruptions occur, public understanding is often limited, making perception easy to manipulate.

Communications Infrastructure and the Information Paradox

Communications infrastructure occupies a unique position in information warfare. It is both a target and a medium.

In Ukraine, attacks on communications networks were accompanied by narratives claiming total isolation, even when partial connectivity remained. These claims intensified fear and hindered coordination, despite technical realities being more nuanced.

At the same time, intact communications networks were used to spread disinformation at scale. Social media platforms, messaging apps, and online forums became battlegrounds where narratives competed in real time.

Railway infrastructure in Vinnytsia, Ukraine — illustrating the vital transport networks that have continued operations despite targeted attacks. Source: George Chernilevsky / Wikimedia Commons, CC BY-SA 4.0

This paradox underscores a challenge for infrastructure protection: connectivity increases both resilience and vulnerability. Robust communications enable coordination and recovery, but they also accelerate the spread of false information.

Managing this tension requires proactive planning rather than reactive moderation.

AI and the Acceleration of Influence Operations

Ukraine has also demonstrated how artificial intelligence and automation are reshaping information warfare. Disinformation campaigns increasingly rely on AI-assisted tools to generate content, translate messages, and adapt narratives rapidly.

These tools enable influence operations to:

- Respond to incidents in near real time
- Tailor messaging to specific regions or communities
- Test and refine narratives at scale
- Sustain high-volume campaigns with limited human input

For infrastructure operators and authorities, this creates a speed asymmetry. Traditional communication processes, often cautious and hierarchical, struggle to compete with automated disinformation systems optimised for velocity rather than accuracy.

As AI-enabled influence operations proliferate, the gap between incident occurrence and narrative dominance will continue to shrink.

Countering Infrastructure-Focused Disinformation: Lessons from Ukraine and the International Response

While Ukraine's experience highlights the risks posed by coordinated information warfare, it also offers important insights into how states and institutions can respond. Over the course of the conflict, Ukraine – often with support from international partners – has developed a set

Community resilience hub ("Points of Invincibility") in Ukraine — illustrating adaptive infrastructure that provides heat, power, and connectivity during outages. Source: Ministry of Digital Transformation / Government of Ukraine.

of adaptive practices aimed at mitigating the impact of misinformation and disinformation surrounding critical infrastructure.

One of the most important developments has been the deliberate integration of strategic communications into infrastructure resilience and crisis management. Ukrainian authorities increasingly treated public communication as an operational necessity rather than a secondary or reputational concern. During major attacks on the energy system, for example, government officials and grid operators provided frequent, transparent updates on outages, repair timelines, and system stability – even when information was incomplete. This approach reduced uncertainty and limited the space available for hostile narratives to dominate the information environment.

Energy sector coordination has been particularly notable. Ukraine's transmission system operator and energy ministry worked closely to ensure that technical messaging, public guidance, and security communications were aligned. Consistent terminology and shared situational awareness helped prevent contradictory statements that could be exploited by disinformation actors. Similar coordination was observed between rail operators and government authorities following attacks on transportation infrastructure, ensuring that service disruptions were explained accurately and proportionately.

Ukraine also made extensive use of trusted intermediaries. Municipal authorities, emergency services, and local infrastructure operators were empowered to communicate directly with communities, reinforcing national messaging with localised, context-specific information. This distributed communication model proved more resilient than reliance on a single centralised voice, particularly when adversaries sought to discredit national institutions.

At the international level, Ukraine benefited from intelligence and information sharing with partner governments and multilateral organisations. Early warning of coordinated disinformation campaigns – particularly those linked to major infrastructure attack waves –allowed authorities to anticipate false narratives and prepare counter-messaging in advance. Diplomatic engagement also played a role, with partner governments publicly rebutting false claims aimed at international audiences regarding Ukrainian infrastructure stability and energy security.

Cooperation with technology platforms formed another layer of response. While not eliminating disinformation, collaboration improved the identification and disruption of coordinated inauthentic behaviour, particularly during periods of intense infrastructure disruption. This included rapid takedowns of networks amplifying false claims about nationwide grid collapse or fabricated secondary hazards.

Beyond Ukraine, a broader international response is emerging. Several countries have established dedicated counter–foreign information manipulation units within national security or communications structures, many of which now explicitly include critical infrastructure within their remit. Regional organisations and alliances have expanded information-sharing mechanisms focused on disinformation trends related to energy, transportation, and emergency response,

reflecting recognition that influence operations often target multiple states simultaneously.

Importantly, these efforts underscore a growing consensus: countering infrastructure-focused disinformation is not solely the responsibility of media regulators or technology companies. It requires sustained collaboration among infrastructure operators, security agencies, regulators, emergency managers, and communicators. Technical resilience and narrative resilience are increasingly understood as interdependent.

Rethinking Resilience: Practical Implications

Ukraine's experience points to a fundamental shift in how critical infrastructure resilience must be understood.

First, disinformation should be treated as an all-hazards threat. It can amplify the impact of any disruption, regardless of cause. Risk assessments that ignore the information domain underestimate vulnerability.

Second, crisis communications must be integrated into infrastructure protection planning. Communication is not merely a public relations function; it is an operational capability that influences safety, compliance, and recovery.

Third, cross-sector collaboration is essential. Disinformation campaigns rarely target a single sector in isolation. Energy, transportation, water, communications, and government institutions are often targeted simultaneously. Information sharing across sectors improves situational awareness and response.

Ukrainian President Volodymyr Zelenskyy with European Commission President Ursula von der Leyen during an EU–Ukraine summit, representing enduring diplomatic engagement on infrastructure, security, and resilience. Source: Wikimedia Commons, CC BY-4.0.

Fourth, leadership awareness matters. Executives, operators, and incident commanders must understand how their actions, statements, and silences can be exploited. Training should include information threat scenarios alongside technical exercises.

Finally, coordination with public authorities and international partners enhances resilience. Influence operations often operate across borders, requiring shared understanding and collective response.

Protecting the Invisible Layer

The war in Ukraine has revealed that critical infrastructure has an invisible layer: public trust, institutional credibility, and shared understanding of reality. This layer is neither purely technical nor purely social, yet it underpins the functioning of every infrastructure system.

Information warfare targets this layer directly. By manipulating perception, adversaries can turn infrastructure incidents into strategic crises without increasing physical damage.

For critical infrastructure protection professionals worldwide, the implication is clear. Resilience is not achieved solely through stronger defences or faster repairs. It also depends on the ability to recognise, anticipate, and counter hostile narratives.

Ukraine's experience offers a stark lesson – but also an opportunity. By learning how information warfare operates in conjunction with infrastructure attacks, societies can strengthen resilience before future crises occur. The alternative is to repair systems repeatedly while the foundations of trust continue to erode.

Beyond Compliance: Conceptual and Implementation Cycles in Critical Infrastructure Protection

By Michael Kolatchev, Principal, Rossnova Solutions & Lina Kolesnikova, Senior consultant, Rossnova Solutions, Belgium

Protection of critical infrastructure (CI) is a core national security responsibility that cannot be ensured by any single actor and therefore requires sustained national-level coordination. As a result, it has become a strategic public policy priority in many states. Although CI protection involves multiple public and private stakeholders, international practice confirms the central role of the state in providing strategic direction, ensuring policy coherence, and integrating security considerations, particularly in response to hybrid threats and malicious activities.

Given the systemic and cross-sectoral nature of CI-related risks, the state typically acts as the principal coordinator by establishing governance structures, adopting national strategies, defining mandatory security and resilience requirements, and overseeing their implementation. Effective CI protection enhances resilience, deterrence, and strategic stability by reducing vulnerabilities

to disruption and coercion, while avoiding unnecessary centralisation of operational functions.

CI protection cannot be achieved through a single decision or strategy. Resource, expertise, and time constraints, combined with evolving infrastructures, societal needs, and threat landscapes, render one-off approaches insufficient. CI protection should therefore be understood as an iterative and adaptive process rather than a fixed objective. National CI frameworks usually require several years to develop and should allow for periodic updates, for example every three to five years, enabling continuity within a coherent framework.

Such an approach requires continuous coordination, information sharing, and education of stakeholders and society. Static measures, including legislation or information websites alone, are insufficient. Information on requirements and planned changes must remain accessible, current, and actively communicated. Ultimately, effective CI protection depends on the feasibility of objectives and strategies relative to national preparedness and, critically, on people. Responsible behaviour and long-term cultural change among key stakeholders and society are essential to sustainable CI protection.

Cycles in the Development of CIP

Experience across jurisdictions suggests that the development of critical infrastructure protection (CIP) can be structured around two interrelated cycles: a strategic conceptualization cycle and a practical implementation

cycle. Their iterative interaction enables continuous adaptation of CIP systems and alignment between strategic objectives and operational outcomes.

The conceptualization cycle covers the formulation, review, and adjustment of CIP strategy. Over time, strategies typically become more refined and aligned with implementation capacities. Maintaining consistency between strategic ambitions and available resources is essential, as persistent misalignment may undermine institutional credibility and stakeholder trust.

A key output of conceptualization is an effective legal and regulatory framework. Legislation should be treated as an integral component of CIP strategy and a tool for its enforcement. The choice of legislative model — umbrella or sector-specific — should reflect institutional maturity and stakeholder compliance capacity. Given the dynamic threat environment, legal frameworks must allow regular adaptation without requiring comprehensive redesign, balancing stability with flexibility.

Conceptualization of the CIP Strategy

The conceptualization of a critical infrastructure protection (CIP) strategy can be understood as an iterative process in which each cycle produces answers to a set of core strategic questions. Where necessary, these answers are formalised through legal and regulatory instruments in order to ensure implementation and accountability. Together, these questions define the key dimensions of CIP strategy development:

- What?
- Who?
- How?
- When?

These dimensions structure strategic decision-making and link policy objectives with governance, operational capabilities, and timelines.

Dimension Key Question Strategic Focus

C.1.1 - What?

Definition of what constitutes critical infrastructure, including

sectors, assets, functions, and services. Identification of protection objectives and priorities, including the balance between protection and resilience. Determination of system boundaries, external dependencies, and relevant threat categories.

C.1.2 - Who?

Allocation of roles and responsibilities among state authorities, regulators, operators, and other stakeholders, including responsibility for strategy development, implementation, coordination, oversight, and effectiveness assessment.

C.1.3 - How?

Selection of protection approaches and instruments, including risk assessment methods, security and resilience measures, operational readiness requirements, coordination mechanisms, and capacity-building. Assessment of the ability of the state and operators to implement these measures.

C.1.4 - When?

Establishment of timelines for strategic decisions, implementation phases, entry into force of requirements, evaluation cycles, and periodic review and adjustment of the strategy and regulatory framework.

Taken together, these dimensions ensure that CIP strategies are not limited to declarative objectives, but are grounded in governance structures, operational feasibility, and temporal discipline — factors that are essential for managing systemic security risks and maintaining strategic stability.

One of the key techniques useful in both formulating the concept and verifying its coherence and feasibility is backward planning and dependency analysis. It starts from the end – imagine, the objective is achieved – and analyses what that future looks like, how that future must function, who does what, etc. Then the analysis goes further backwards finding which necessary components of the future should become available and by when, etc.

Outcomes of Conceptualization and link to Implementation

The outcome of conceptualization is typically formalised in a roadmap defining strategic objectives, timelines, and means. Each conceptualization cycle may encompass multiple implementation cycles aimed at building and sustaining CIP capabilities. This approach enables anticipation of future requirements while ensuring alignment between near-term actions and long-term objectives.

Given evolving threats and constraints, both conceptual and implementation frameworks must adapt over time. Legal and regulatory instruments should therefore support adjustment without undermining legal certainty—an essential requirement in a national security context.

Implementation Cycles

Implementation cycles translate strategic intent into operational reality and provide the feedback necessary for subsequent refinement of the CIP strategy. Multiple implementation cycles may be executed within a single conceptualization cycle, allowing strategic priorities to be pursued through phased, resource-constrained actions.

Each implementation cycle can be structured around four core processes:

- **Planning** – identification of priority sectors, assets, functions, risks, and acceptable disruption thresholds; development of policies, procedures, response plans, performance indicators, and resource allocation mechanisms.
- **Implementation** – execution

CONNECT WITH US AT CIPRNA 2026

SIPS & SURVEILLANCE

EAT + DRINK + CONNECT
PLUS, LEARN HOW TECHNOLOGIES UNITE TO PROTECT SITES FROM DRONES.

LONG-DISTANCE SURVEILLANCE

UNIFIED PLATFORM

PRECISION RADAR

REGISTER WITH CODE: AXIS-GUEST

WHEN
WEDNESDAY, MARCH 11TH
@ 5:30PM

WHERE
CROWNE PLAZA,
BATON ROUGE, LA

Genetec™ AXIS COMMUNICATIONS ECHODYNE

of technical, organisational, and administrative measures, including security enhancements, monitoring, training, redundancy development, exercises, and testing.

- Verification and Evaluation – assessment of effectiveness and compliance through audits, monitoring, testing, exercises, and incident analysis; identification of gaps, deficiencies, and deviations from planned outcomes.
- Improvement and Adaptation – implementation of corrective and preventive actions, adjustment of plans and architectures, scaling of effective solutions, and incorporation of lessons learned into subsequent cycles.

Each implementation cycle is time-bound, reflecting budgetary and resource constraints, while the operation of the protection system itself remains continuous. The use of multiple, iterative cycles enables earlier learning, timely scaling of successful measures, and adjustment of strategy in response to evolving threats.

At the same time, the adaptive capacity of implementation cycles is fundamentally shaped by the objectives, priorities, and boundaries defined during conceptualization. In this sense, conceptualization serves as a strategic constraint and enabler for operational flexibility, directly influencing the effectiveness of CIP as an instrument of national security and resilience.

Wrapping up and drawing from experience

The conceptualization cycle plays a decisive role in defining the objectives, principles, architecture, and core mechanisms of critical infrastructure (CI) protection. Each cycle results in an agreed set of strategic objectives and a corresponding strategy for their achievement, while establishing the parameters that guide subsequent implementation cycles.

Within this process, the definition of objectives — the "what" dimension (C.1.1) — is of central importance. Objectives are rarely fixed at the outset and may be revised multiple times within a single cycle based on analysis across the remaining dimensions: "who" (C.1.2), "how" (C.1.3), and "when" (C.1.4), which reflect governance structures, available instruments, and temporal constraints. As a result, conceptualization typically proceeds through iterative adjustments that align strategic intent with feasibility and capacity.

This iterative logic enhances strategic coherence and realism, reducing the risk of setting objectives that are unattainable or disproportionate to available resources—a common source of failure in national security policy design.

Drawing on international practice, several core recommendations can be identified for the development of CI protection systems:

Conceptualization cycle

- Clearly define the scope of protection, prioritising critical functions and services and accounting for cascading and cross-border dependencies.
- Establish a clear allocation of roles and responsibilities among state authorities, operators, and other stakeholders, supported by central coordination.
- Develop a realistic strategy aligned with national capabilities, resources, and an adaptive legal and regulatory framework.

Implementation cycles

- Apply phased, time-bound implementation with achievable objectives and measurable outcomes.
- Ensure coordination mechanisms capable of operating in both routine and crisis conditions.

- Institutionalise regular testing and exercises as a core element of resilience and readiness.

Cross-cutting principles

- Embed continuous feedback and improvement through the integration of implementation results into governance and strategic review.
- Maintain transparency and predictability of requirements while avoiding excessive or purely formal regulation.
- Prioritise resilient and reliable operation over formal compliance, treating day-to-day system performance as the primary measure of effectiveness.

While international experience provides valuable guidance, its effectiveness depends on careful adaptation to national legal frameworks, institutional arrangements, infrastructure maturity, and resource constraints. In a security context, successful CI protection is achieved not through replication of external models, but through the disciplined translation of international best practices into nationally viable strategies.

Policy Implications and Initial Steps

As initial steps toward the development of a national concept and legal framework for critical infrastructure (CI) protection, states should adopt a risk-governance–driven approach grounded in an explicit understanding of the evolving threat environment. Priority actions include:

- conducting a systematic inventory of infrastructures, functions, and services

based on their criticality, interdependencies, and potential national-level impact under diverse threat scenarios;

- assessing maturity and readiness of key operators and public authorities to manage risks arising from cyber, physical, hybrid, and systemic disruptions;
- defining core principles and strategic priorities for CI protection that reflect national risk tolerance, security objectives, and available capabilities and resources;
- defining (estimating) the pace of continuous CIP build-up as the country and the society can realistically afford, with, for example, 3-or 5-year iterations;
- developing a framework concept and roadmap that enable phased implementation and adaptive responses to changing threat dynamics;
- initiating preparation or adaptation of legal and regulatory instruments designed to support continuous risk assessment, feedback, and periodic revision of requirements.

Together, these steps provide the institutional and analytical foundation for integrating CI protection into broader national security risk governance and resilience planning, while staying realistic and adequate to individual country situation, balancing the “would” with the “could”.

CISA Unveils Enhanced Cross-Sector Cybersecurity Performance Goals

The Cybersecurity and Infrastructure Security Agency (CISA) released version 2.0 of its Cross-Sector Cybersecurity Performance Goals (CPGs), offering organizations a more robust framework for integrating cybersecurity into daily operations. The updated CPGs align with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0, incorporates three years of operational insights, and address emerging threats through data-driven, actionable guidance. These enhancements are designed to promote accountability, improve risk management, and support strategic cybersecurity governance across sectors.

The Cross-Sector CPGs represent a targeted subset of best practices, carefully selected through extensive consultation with industry leaders, government stakeholders, and cybersecurity experts. Designed to meaningfully reduce risks to critical infrastructure and safeguard the American public, these goals offer a practical starting point for small and medium-sized organizations. By focusing on a limited set of high-impact actions, the CPGs help prioritize cybersecurity investments that deliver measurable improvements in resilience and risk reduction.

The updated goals offer expanded and clarified guidance across key cybersecurity domains—including account and device security, data protection, governance, vulnerability management, supply chain risk, and incident response and recovery. Building on the foundation of version 1.0.1, CPG 2.0 introduces several notable improvements:

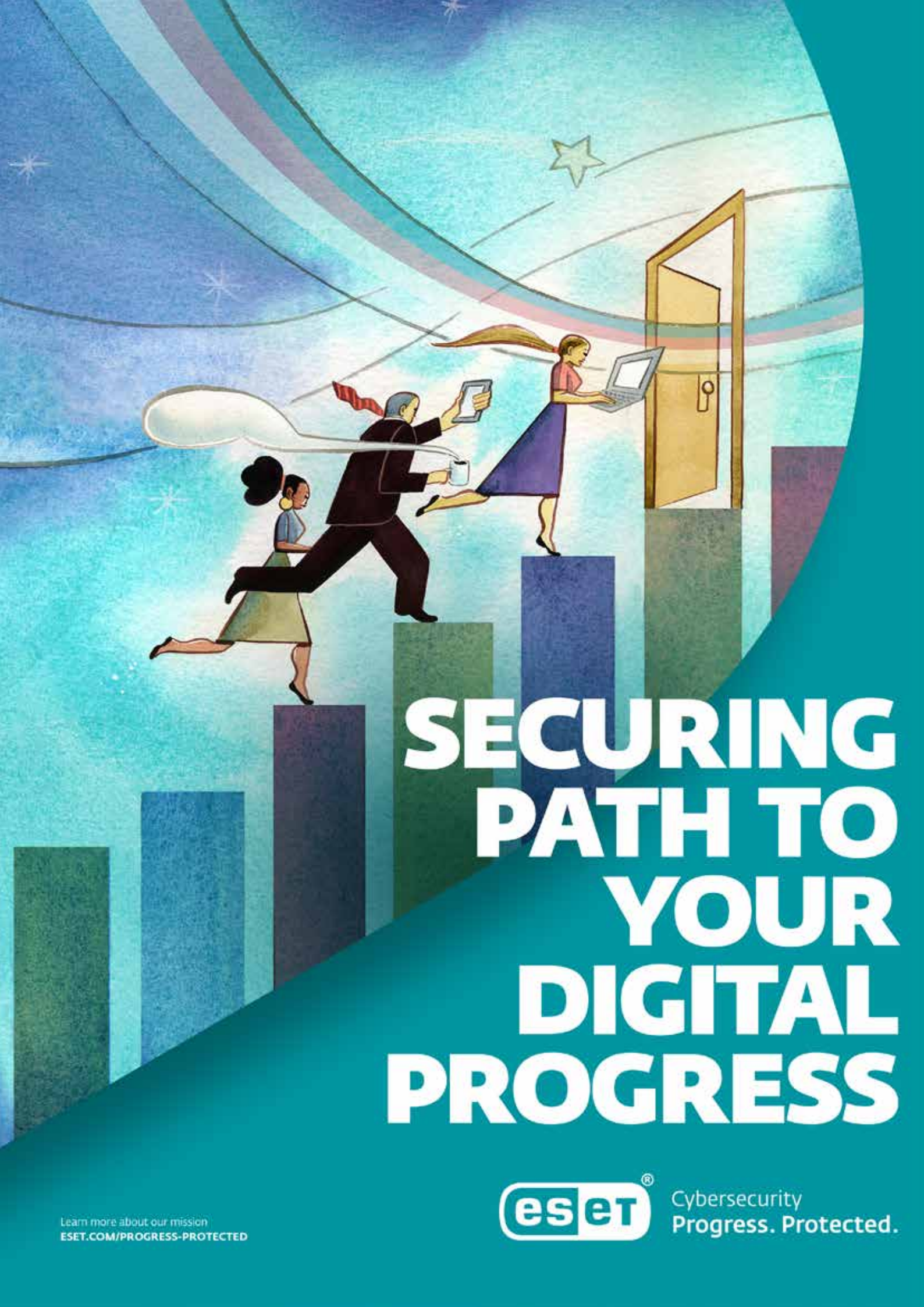
- **Governance Emphasis**: A new "Govern" function underscores the critical role of organizational leadership in cybersecurity, regrouping existing goals and introducing two new ones focused on risk management strategy, policy development, and executive accountability.
- **Unified Goal Structure:** Operational Technology (OT) and Information Technology (IT) goals are now consolidated into universal goals, eliminating silos across IT, Internet of Things (IoT), and OT environments.
- **Threat-Responsive Expansion:** New goals address emerging threats, third-party risk, zero trust architecture, and incident communication protocols.
- **Streamlined Framework:** Redundant, unclear, or underutilized goals have been removed to improve clarity and usability.
- **Enhanced Documentation:** Each goal now includes clearer methodology and supporting materials to reduce guesswork and improve implementation.

"Over the past year, CISA has engaged extensively with hundreds of stakeholders across both the public and private sectors to ensure the updated goals reflect real-world challenges and operational realities," said Madhu Gottumukkala, Acting CISA Director. "Version 2.0 demonstrates our commitment to listening to and incorporating partner feedback to deliver practical, outcome-driven guidance that organizations can act on. These goals are applicable across all critical infrastructure sectors and offer foundational protection for organizations regardless of their cybersecurity maturity. We encourage all organizations to adopt the new CPGs and continue sharing feedback to help us refine future iterations."

The Cross-Sector CPGs serve three primary purposes:

- **Provide measurable actions** that critical infrastructure entities can take to achieve a basic level of cybersecurity.
- **Bridge communication gaps** between IT/OT technical staff and organizational leadership to align on cybersecurity priorities.
- **Support strategic planning** by offering clear guidance that informs both near- and long-term cybersecurity investments.

CISA encourages organizations to adopt the voluntary Cross-Sector CPGs. To learn more about the updated Cybersecurity Performance Goals and how they can support your organization's cybersecurity program, visit Cross-Sector Cybersecurity Performance Goals and Objectives.



SECURING PATH TO YOUR DIGITAL PROGRESS

Learn more about our mission
ESET.COM/PROGRESS-PROTECTED

ESET®
Cybersecurity
Progress. Protected.

Creating Security and Resilience for Critical Infrastructure

By Annie McIntyre, Chief Security Officer, EverLine – Energy's Technical Stack

When it comes to cyberterrorists, adversaries have become more focused, methodical, and strategic, advancing much more quickly than ever before. It's corporate suicide to underestimate them.

The shifting landscape of cyberthreats is so profound that it has created its own vernacular. Examples of new cyber terms include:

- Breakout time — the amount of time it takes for an adversary to move laterally across a network reached an all-time low in 2024. The average breakout time was 48 minutes; the fastest was 51 seconds.
- Voice phishing (vishing) attacks – a tactic where adversaries call victims to amplify their activities with persuasive social engineering techniques.
- Smishing – utilizing the SMS or text messages as a phishing technique. This often involves convincing the user to give up credentials or information or perform a task useful to the adversary.
- Access-as-a-Service (AaaS) – an underground business economy where cybercriminals

sell access to compromised networks to less-skilled attackers, enabling them to deploy malware, ransomware, or other attacks without doing the initial compromise themselves. It commoditizes initial intrusion, making sophisticated attacks accessible to almost anyone. By significantly lowering the barrier to entry, AaaS increases the volume and sophistication of global cyber threats.

For decades, cybersecurity in critical infrastructure was based on corporate risk-reduction initiatives rather than regulatory compliance.

U.S. critical infrastructure regulations did not include cybersecurity elements until NERC CIP in 2008. The Transportation Security Administration Security Directives arrived in 2021, a marked departure from federal guidelines and recommendations to requirements. Incident reporting for specific infrastructure sectors became a requirement in the last few years.

There are now sector-specific regulations for pipelines, rail, and maritime, which involve key agencies such as TSA and USCG that issue rules for mandatory Cyber Risk Management (CRM) programs, including incident reporting, developing Cybersecurity Plans (like CIP for pipelines/rail, and USCG plans for maritime), appointing security officers with specific cyber responsibilities, conducting assessments, and implementing countermeasures to protect against threats – all of which mandate specific actions, timelines for implementation, and integration of IT/OT security,

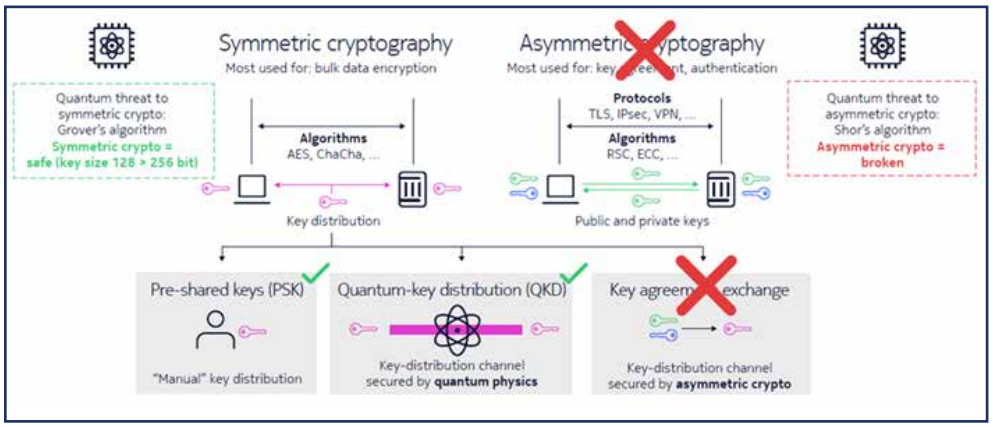


Figure 1: Symmetric and asymmetric cryptography

supply chain risk, and physical security coordination.

Insurers, customers, partners, and investors have a vested interest in compliance and expect clean audit results and tangible evidence that security controls are in effect, and the entity is committed to maintaining a resilient security and compliance program.

Threats targeting critical infrastructure are well-publicized due to the significant strategic risks they pose to national security, economic prosperity, and public safety. With best practices to protect against threats readily available, asset owners have a legal and ethical obligation to be informed and take proactive measures to mitigate them. Pleading ignorance is not a valid defense for noncompliance. That said, protecting essential services is not always easy. Established adversaries continually identify new targets and add more sophisticated techniques to their arsenals for evasion, intrusion, and exfiltration, and the number of named adversaries continues to expand.

The breadth and depth of cybercriminals' technical skills, industry knowledge, and recent successful incidents have motivated federal regulators and states to ensure that all sectors employ security measures, including cyberinsurance and regular cyber training.

Although landing a whale may be ideal, more than 40% of cyberattacks target small- to medium-sized organizations. Cybercriminals view smaller entities as easier prey due to perceived smaller budgets and weaker security, making robust defenses and employee training crucial for survival.

The cybersecurity landscape continues to evolve rapidly, presenting significant challenges for organizations across sectors and geographies. As long as there are benefits, adversaries will explore new initial access methods to bypass security defenses – and their resilience, innovation, and adaptability will underscore the critical need for a comprehensive understanding of threats across every aspect of the landscape.

The notable themes, trends, and events spreading across the cyber threat landscape require anticipatory threat assessments to help prepare and protect organizations throughout

the coming year. It requires a comprehensive understanding of today's threats across every aspect of the landscape.

Adversaries will also continue to use methods, even basic tactics, for as they continue to be successful. Without solid countermeasures, even basic phishing can create a disaster. Organizations must protect against a spectrum of threats and their capabilities.

Secure the entire identity ecosystem:

Credential theft, Multi-Factor Authentication (MFA) bypass, and social engineering provide cybercriminals with cover to move laterally across on-premises, cloud, and SaaS environments via trusted relationships. By impersonating legitimate users, they can escalate access and evade detection. Criminals can be deterred by adopting phishing-resistant MFA solutions and access policies to prevent unauthorized access, including just-in-time access, regular account reviews, and conditional access controls.

Threat detection tools that monitor behavior across endpoints and on-premises, cloud, and SaaS environments will flag privilege escalation, unauthorized access, or backdoor account creation. Integrating them with Extended Detection and Response (XDR) platforms provides comprehensive visibility and a unified defense against adversaries. In addition, users should be educated to recognize vishing and phishing attempts while maintaining proactive monitoring to detect and respond to identity-based threats.

By taking core principles from Sun Tzu's "Art of War" organizations are well-advised to understand the opponents' strengths, weaknesses, tactics, and motivations. Coupling that knowledge with self-awareness is crucial for strategic success in conflict, including cyberwarfare. Preparation involves gathering intelligence on threats, assessing internal capabilities, and devising strategies to secure any vulnerabilities while mitigating risks.

Create a unified security platform that integrates data from endpoints, cloud, and identity systems

The growing popularity of living-off-the-land methods that utilize standard services and legitimate tools is making threat detection tougher and response slower. Unlike traditional malware, these approaches give attackers the ability to bypass traditional security measures by executing commands and using legitimate software to mimic normal operations.

Effective neutralization of attacks requires modernization of detection and response strategies. AI-based monitoring, XDR and next-generation Security Information and Event Management (SIEM) solutions offer integrated visibility across endpoints, networks, cloud environments, and identity systems. This integration enables analysts to correlate suspicious behaviors and view the complete attack path.

Detection can be further enhanced by refining "normal" behavior, identifying potential attack patterns, and providing insights into adversary tactics, techniques, and procedures. With real-time intelligence, organizations can stay informed about emerging threats, anticipate attacks, and prioritize critical security efforts.

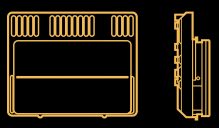
Defend core cloud infrastructure

Although many infrastructure organizations are using cloud technology, it must be used with caution. Operability in the cloud, especially for core and critical services, must undergo a risk assessment, careful implementation, and maintenance. The cloud comes with risks, and those may be too much for highly critical operations.

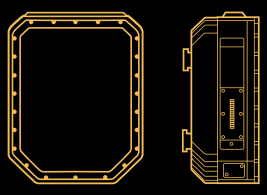
Improve Security Resilience with Radar

Fill security gaps and improve operational efficiency. Accurately detect and track ground and air threats, including dark drones.

EchoGuard®



EchoShield®



Radar for Critical Infrastructure Protection

ECHODYNE

RADAR REINVENTED™

Adversaries targeting cloud environments exploit the complexity of cloud infrastructure by focusing on three primary attack vectors: misconfigurations, stolen credentials, and the abuse of legitimate cloud management tools. These tactics allow them to infiltrate systems, navigate laterally across networks, and maintain persistence for activities such as data exfiltration and the deployment of ransomware.

Countering cloud-based threats with cloud-native application protection platforms (CNAPPs) that include cloud detection and response (CDR) capabilities can provide operators with a unified view of their cloud security posture and help rapidly detect, prioritize, and remediate misconfigurations, vulnerabilities, and adversary threats. Implementing robust policies and technical measures to ensure only authorized users can assess specific resources limits exposure to critical systems and ensures continuous monitoring for anomalies, including logins from unexpected locations.

Also important are regular audits to proactively locate any vulnerabilities before attackers do. Automated tools can uncover overly permissive storage settings, exposed APIs, and unpatched vulnerabilities. And regular reviews of cloud environments are a critical security practice for managing access and configuration settings which minimizes attack surfaces, addresses outdated configurations, and implements least privilege.

Go beyond technical vulnerabilities – take an adversary-centric approach

Published vulnerabilities that remain unaddressed can present significant opportunities for adversaries in any environment. A single exploited vulnerability presents a world of options for an adversary, especially if they remain undetected. They can cascade and create chaining, which combines multiple vulnerabilities to gain rapid access, escalate privileges, and bypass defenses. Multi-stage attacks in common vulnerabilities and exposures (CVEs) often fall on public resources like Proof-of-Concept (POC) exploits and technical blogs which give adversaries the opening to rapidly develop effective and hard-to-detect payloads.

Countering them requires systematic patches or upgrades of critical systems, especially internet-facing services like web servers and VPN gateways. By understanding and monitoring for anomalies, privilege escalation attempts, and other subtle signs of exploit chaining can provide detection for large-scale attacks before they advance into full-scale attacks.

Know your adversary and be prepared

When facing any advisory, preparation is key. Understanding potential attackers, whether nation-states, criminals, or hacktivists, and knowing their motives and their Tactics, Techniques, and Procedures (TTPs) moves organizations from reactive to proactive security when building defenses against them. Threat intelligence, advisory profiling, and tradecraft analysis helps mitigate blind spots when prioritizing resources, adapting defenses, and stop threats before they escalate.

Conclusion

Cyberattacks can happen at breakneck speed. From the initial point of entry, an attacker can infiltrate through automated scans almost instantly. Once initial access is gained, the breakout time can take as little as minutes or as long as hours. Once access is gained, it can take just moments for hackers to deploy ransomware.

In contrast, it takes most organizations an average of 181 days to identify a data breach, and an additional 60 days to contain it.

Being prepared can make the difference between containment

and catastrophe. By taking intelligence-driven approaches, security teams can move an organization beyond reactive defense to anticipating and preventing them.

Technology will also play a critical part in detecting and stopping intrusions, yet end users remain a critical link in the chain to stop breaches. Coupling technologies with practices that strengthens the human link, organization can mitigate the vulnerabilities and effectively shut down the adversary. In time, adversaries find it inefficient to keep trying and they move on. Attempts will never cease, but organizations can rest easier knowing they are prepared, defenses are in place, and they have a confident view of their architecture.

Annie McIntyre is Chief Security Officer at EverLine. Prior to EverLine, McIntyre was the President and Chief Executive Officer of Ardua Strategies, Inc., a Texas Corporation, providing solutions for the cyber and operational security issues of energy and infrastructure. Ardua was acquired by EverLine in 2021.

McIntyre conducts extensive work on security policies as they relate to energy and infrastructure. She serves on the Advisory Council at the North American Energy Standards Board, is a Board Member of the Mission Critical Global Alliance and has served as a Senior Fellow at the University of Minnesota's Technology Leadership Institute.

New Joint Guide Advances Secure Integration of Artificial Intelligence in Operational Technology

The Cybersecurity and Infrastructure Security Agency and the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), in collaboration with U.S. and international government partners, has published Principles for the Secure Integration of Artificial Intelligence (AI) in Operational Technology (OT). This joint guide provides four key principles that will help critical infrastructure OT owners and operators mitigate unique risks and achieve a balanced integration of AI into OT environments.

"AI holds tremendous promise for enhancing the performance and resilience of operational technology environments – but that promise must be matched with vigilance," said CISA Acting Director Madhu Gottumukkala. "OT systems are the backbone of our nation's critical infrastructure, and integrating AI into these environments demands a thoughtful, risk-informed approach. This guidance equips organizations with actionable principles that AI adoption strengthens—not compromises—the safety, security, and reliability of essential services."

This joint guide provides key principles that will help critical infrastructure owners and operators safely and effectively integrate AI into OT systems. The four key steps are:

1. Understand AI: Educate personnel on AI risks, impacts, and secure development lifecycles.

2. Assess AI Use in OT: Evaluate business cases, manage OT data security risks, and address immediate and long-term integration challenges.

3. Establish AI Governance: Implement governance frameworks, test AI models continuously, and ensure regulatory compliance.

4. Embed Safety and Security: Maintain oversight, ensure transparency, and integrate AI into incident response plans.

"The integration of AI into critical infrastructure brings both opportunity and risk," said Nick Andersen, Executive Assistant Director for Cybersecurity. "While AI can enhance the performance of OT systems that power vital public services, it also introduces new avenues for adversarial threats. That's why CISA, in close coordination with our U.S. and international partners, is committed to providing clear, actionable guidance. We strongly encourage OT owners and operators to apply the principles in this joint guide to ensure AI is implemented safely, securely, and responsibly."

This joint guide focuses on machine learning (ML)- and large language model (LLM)-based AI, and AI agents. However, this guidance may also be applied to systems augmented with traditional statistical modeling and other logic-based automation.

CIP-014-4 Is Expanding the Physical Security Perimeter: What Municipally Owned Utilities Must Prepare for Now

Rob Velasco, President, CIP Global Ventures, and Jen Russell, SVP and Co-Founder, EAGL Technology

Introduction: A Quiet but Significant Shift

For more than a decade, NERC Critical Infrastructure Protection (CIP) standards have shaped how electric utilities approach cybersecurity and physical security. Historically, the most stringent requirements applied primarily to large Investor-Owned Utilities (IOUs) operating high-voltage Bulk Electric System (BES) assets at 500 kV and above. Municipally owned utilities, public power districts, and smaller transmission owners often operated adjacent to — but outside of — the strictest regulatory perimeter.

That line is now shifting.

Anticipated changes associated with CIP-014-4 signal a material expansion in how critical substations are identified, assessed,

and protected — particularly for assets operating in the 200 kV to 499 kV range. For many municipally owned utilities, this may be the first time their substations fall squarely within the scope of CIP-014's physical security planning, risk assessments, and mitigation obligations.

This article is intended as a practical heads-up for municipal and public power leaders. It explains how CIP-014 intersects with existing standards such as CIP-006, why traditional perimeter protection alone is insufficient, and how modern, integrated physical security technologies can help utilities protect, detect, and deter real-world threats — without overwhelming Security Operations Centers (SOCs) or operations staff.

From CIP-006 to CIP-014: Why the Scope Is Changing

Many municipal utilities are already familiar with CIP-006, which focuses on physical security of BES cyber systems—specifically control rooms, operational buildings, and other facilities that house BES cyber assets. CIP-006 emphasizes:

- Controlled physical access
- Visitor logging and escorting
- Monitoring of access points
- Physical protection of BES Cyber System locations

What CIP-006 does not fully address is the broader substation yard and the critical physical assets within it, such as transformers, breakers, capacitor banks, and battery enclosures—assets whose destruction or degradation could have wide-area reliability consequences even if cyber systems remain intact.

This is where CIP-014 becomes fundamentally different.

CIP-014 requires utilities to:

1. Identify transmission stations and substations whose loss could result in widespread instability, uncontrolled separation, or cascading outages, and
2. Develop and implement physical security plans to protect those facilities against physical threats.

As voltage thresholds and risk-based methodologies evolve, substations previously treated as "distribution-adjacent" or secondary transmission assets may now qualify as critical under CIP-014-4, particularly in dense urban environments or regions with constrained redundancy.

For municipal utilities, this often means:

- Assets once managed under CIP-006 assumptions are now subject to perimeter-level physical security planning
- Existing protection strategies may be necessary but no longer sufficient
- Physical security must extend beyond buildings to yard-level critical equipment

The Scale of the Challenge: Thousands of Substations, New Expectations

The U.S. electric grid includes more than 55,000 substations, the majority of which have never been subject to CIP-014 requirements. While only a subset of these will ultimately qualify as CIP-014 critical facilities, the number is still significant—especially for municipal utilities operating regional transmission assets in the 200–499 kV range.

Unlike large Investor-Owned Utilities with centralized security teams and long CIP compliance histories, many municipal utilities face:

- Lean staffing models
- Limited in-house physical security expertise
- Legacy infrastructure designs never intended to withstand modern threat vectors

The result is a compliance and security gap—not due to negligence, but due to changing risk realities.

Why Concrete Walls Alone Are No Longer Enough

A common first response to physical security concerns is to increase perimeter hardening, often through:

- Taller chain-link fencing
- Anti-climb features
- Concrete or masonry walls

While these measures play an important role, they are not sufficient on their own in the face of today's threat environment.

Modern adversaries increasingly rely on:

- High-powered rifles, including AK- and AR-platform weapons
- Elevated firing positions outside the fence line
- Long-range standoff attacks targeting exposed equipment

Almost every substation in the United States includes elevated points of interest — nearby overpasses, buildings, hills, or natural terrain — that allow adversaries to fire over perimeter fencing or walls.

A 12-foot concrete wall does little to protect a transformer radiator, bushing, or control cable tray from a rifle fired hundreds of feet away.

A Modern Physical Security Framework: Protect, Detect, Deter

To meet both the letter and intent of CIP-014, utilities must think beyond perimeter fencing and adopt a layered strategy built on three pillars:

1. PROTECT: Harden What Matters Most

Protection should focus on critical assets within the perimeter, not just the perimeter itself.

For substations newly entering CIP-014 scope, this increasingly includes:

- Power transformers
- Mobile transformer connection points
- Control rooms and CIP-006 buildings
- Battery energy storage enclosures
- Critical communications and protection cabinets

UL 752 Level 8 ballistic-resistant barriers are emerging as a practical solution for this layer. Properly designed, these barriers:

- Stop multiple rounds from high-powered rifles
- Are non-conductive and non-corrosive, suitable for energized environments
- Can be installed very close to assets, preserving airflow for cooling
- Are lightweight enough to be installed, removed, and repositioned by a two-person crew

Unlike permanent concrete structures, modular ballistic barriers can be customized in size and shape, allowing utilities to protect irregularly shaped assets without impeding maintenance or violating clearance requirements.

2. DETECT: Know Immediately When an Attack Occurs

Protection without detection is incomplete.

CIP-014 physical security plans increasingly require utilities to demonstrate the ability to identify and respond to physical attacks in real time. This is where many legacy systems fall short.

Traditional gunshot detection technologies often rely on:

- Single-factor acoustic signatures
- Outdated processing stacks
- Algorithms prone to false positives from construction noise, fireworks, or industrial activity

False alarms overwhelm SOC operators, erode confidence, and slow response times.

Modern approaches — such as multi-factor gunshot detection — address these limitations by:

- Immediately identifying the specific energy signature created by a firearm discharge
- Correlating that energy with the distinct waveform signature created

Help2Protect against the Insider Threat

Insider Threat Awareness and Program Development Training platform

Help2Protect.info

Protect your company from Insider Threats

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

as each caliber moves through the air to increase accuracy in the 99.999%

- Authenticating events before alerts are generated
- Reduction in risk by eliminating the need for "hot microphone" audio sensor technology

This approach dramatically reduces false positives while ensuring genuine threats are escalated immediately.

3. DETER: Change the Adversary's Decision-Making

Deterrence is often overlooked in utility security planning, yet it is one of the most effective ways to reduce risk.

When a ballistic event is detected, advanced systems can:

- Identify the GPS location of the shooter
- Calculate shot trajectory and direction of fire
- Pass that information instantly to deterrent technologies

These deterrents may include:

- Rapid deployment drones
- Ground-based surveillance robots
- Long Range Acoustic Devices (LRADs)
- Automated lighting or audible warnings

The goal is not confrontation — it is disruption. Adversaries who realize they have been detected, tracked, and illuminated are far more likely to disengage before causing catastrophic damage.

The Importance of a Single Pane of Glass

As CIP-014 expands, so does operational complexity.

One of the most consistent challenges reported by SOC operators is tool overload. When an incident occurs, operators cannot afford to:

- Switch between a Video Management System (VMS)
- Open a separate perimeter detection dashboard
- Check a gunshot detection application
- Launch a drone interface
- Access a robot control console

Seconds matter during an active security event.

A unified, single-pane-of-glass architecture allows operators to:

- See alerts, video, sensor data, and response tools in one interface
- Make decisions faster
- Reduce training and operational burden
- Improve compliance documentation and after-action reporting

Equally important, open integration with platforms such as Genetec, Axis Communications, Magos, and others ensures that utilities are not locked into proprietary silos as their security programs evolve.

What Municipal Utilities Should Do Now

For municipally owned utilities potentially entering CIP-014 scope for the first time, preparation should begin well before formal enforcement deadlines.

Key steps include:

1. Re-evaluate existing CIP-006 sites

Determine which facilities may now fall under CIP-014 physical security planning due to voltage level, system topology, or regional criticality.

2. Map critical assets within the substation perimeter

Go beyond transformers — include buildings, enclosures, and supporting infrastructure.

3. Assess ballistic exposure, not just access control

Identify elevated firing positions and long-range sightlines.

4. Prioritize modular, adaptable protection solutions

Avoid designs that limit maintenance access or future upgrades.

5. Invest in detection technologies that reduce false alarms

SOC credibility depends on signal quality.

6. Design deterrence into the plan—not as an afterthought

Deterrence multiplies the value of detection.

7. Insist on integration and interoperability

CIP-014 compliance should simplify operations, not complicate them.

Conclusion: Compliance Is the Floor, Not the Ceiling

CIP-014-4 represents more than a regulatory update—it reflects a recognition that physical attacks on the grid are no longer theoretical. For municipally owned utilities, the challenge is not just compliance, but doing so intelligently, with technologies and architectures that scale, integrate, and perform under real-world conditions.

Protection today is not about a single wall, sensor, or camera. It is about coordinated, real-time awareness—protecting what matters most, detecting threats when they occur, and deterring adversaries before damage is done.

Utilities that begin this work now will not only be better positioned for CIP-014 compliance — they will be more resilient, more confident, and better prepared for the evolving threat landscape ahead.

CISA Unveils Enhanced Cross-Sector Cybersecurity Performance Goals

The Cybersecurity and Infrastructure Security Agency (CISA) launched a new Industry Engagement Platform (IEP) designed to facilitate structured, two-way communication between the agency and companies developing innovative and security technologies. The IEP enables CISA to better understand emerging solutions across the technology ecosystem while giving industry a clear, transparent pathway to engage with the agency.

"With the launch of this new platform, we're opening the door wider to innovation—giving industry a direct line to share the tools and technologies that can help CISA stay ahead of evolving threats," said CISA Acting Director Madhu Gottumukkala. "The private sector drives innovation and this collaboration is essential to our national resilience."

The IEP allows organizations – including industry, non-profits, academia, government partners at all and the research community – with a structured process to request conversations with CISA subject matter experts to describe new technologies and capabilities. These engagements give innovators the opportunity to present solutions that may strengthen our nation's cyber and infrastructure security.

Through customizable technology profiles, the IEP helps connect organizations to the right CISA experts by capturing areas of expertise and specific topics organizations wish to discuss. Participants may also upload capability overviews for CISA to reference in market research and in understanding emerging technologies across sectors.

While participation in the IEP does not provide preferential consideration for future federal contracts, it serves as a key channel for CISA to gain insight into new capabilities and market trends that support mission needs.

CISA encourages organizations with new, emerging, or advanced technology solutions to visit the Industry Engagement Platform. Current areas of interest include:

- Information technology and security controls
- Data, analytics, storage, and data management
- Communications technologies
- Any emerging technologies that advance CISA's mission, including post-quantum cryptography and other next-generation capabilities

"Strategic collaboration is essential to strengthening national security and resilience," Gottumukkala added. "The IEP is one of the ways CISA is aligning innovation with mission needs to advance the defense of our nation's cyber and critical infrastructure."

International Association of
CIP Professionals

CHAIRMAN's 2026 MESSAGE

As we begin a new year, I would like to extend my warmest wishes to all members, friends and associates of the International Association of Critical Infrastructure Protection Professionals (IACIPP) - Happy New Year to you. The start of 2026 offers an opportunity for reflection, renewal, and recommitment to the vital mission that unites us: safeguarding the systems, assets, and services upon which our societies depend.

The past year was one of continued volatility and rapid change. Across energy, transport, water, health, communications, finance, and digital infrastructure, professionals have operated in an environment shaped by converging risks—geopolitical instability, accelerating digital transformation, climate-driven disruptions, and an increasingly complex threat landscape. In this context, the professionalism, resilience, and dedication demonstrated by our members have been nothing short of exemplary. On behalf of the Association, I thank you for your contribution to protecting critical infrastructure and, by extension, public safety and economic stability.

Looking ahead to 2026, it is clear that the challenges facing our industry are not diminishing; rather, they are evolving in both scale and complexity. One of the defining features of the year ahead will be the continued convergence of physical and cyber risk. Digital systems are now deeply embedded in operational technology, supply chains, and decision-making processes. While this integration brings efficiency and innovation, it also expands the attack surface for malicious actors. Cyber-enabled disruption, whether from state-sponsored groups, criminal networks, or ideologically motivated individuals, will remain a persistent concern for infrastructure operators worldwide.

At the same time, geopolitical tensions continue to reshape the global risk environment. Critical infrastructure is increasingly viewed as a strategic target in times of conflict and competition. Hybrid threats—including sabotage, espionage, disinformation, and economic coercion—blur traditional boundaries between peace and crisis. For professionals in our field, this requires not only technical competence but also strong situational awareness, cross-sector collaboration, and an understanding of how global events can manifest as local operational risks.

Climate change and extreme weather events represent another pressing challenge for 2026. Floods, heatwaves, wildfires, and storms are placing unprecedented strain on infrastructure designed for a different climate reality. Resilience is no longer a theoretical concept, it is an operational necessity. Infrastructure protection professionals will be expected to contribute to adaptation planning, continuity strategies, and recovery frameworks that ensure essential services can withstand and rapidly rebound from environmental shocks.

The human dimension of our profession also deserves attention as we enter the new year. Skills shortages, workforce fatigue, and the need for continuous upskilling are becoming more acute across the sector. As technologies advance and threats diversify, the demand for multidisciplinary expertise grows. Investing in people—through training, mentoring, and knowledge-sharing—will be just as critical as investing in systems and technologies. Our Association has a key role to play in fostering professional development and supporting the next generation of infrastructure protection professionals.

In 2026, trust and collaboration will remain central to effective critical infrastructure protection. No single organisation, sector, or nation can address these challenges in isolation. Information sharing, public–private partnerships, and international cooperation are essential enablers of

security and resilience. As an Association, we will continue to promote dialogue across disciplines and borders, providing platforms where professionals can exchange insights, lessons learned, and good practice. This is where events such as the upcoming Critical Infrastructure Protection & Resilience North America (CIPRNA) conference and exhibition in Baton Rouge, Louisianna on the 10th-12th March, provides industry professionals, government agencies and academia a great opportunity to develop their knowledge, understanding and network of experience.

IACIPP's priorities for the year ahead reflect these realities. We will continue to strengthen our professional standards, expand learning opportunities, and provide a platform where like-minded individuals can connect and communicate. We are also committed to ensuring that our guidance and activities remain practical, forward-looking, and grounded in the real-world challenges faced by our members and colleagues.

As we embark on 2026, I encourage each of you to take a moment to reflect on your own role within this broader mission. The work you do matters. Often unseen by the public, your efforts underpin societal resilience, economic continuity, and national security. In a world of uncertainty, your expertise provides stability.

Thank you for your continued engagement with the Association. I look forward to the year ahead and to working together as we navigate its challenges and opportunities.

I wish you a safe, successful, and fulfilling year ahead.

John Donlon QPM FSyI
Conference Chairman
Chairman, IACIPP

Critical Infrastructure Protection & Resilience North America

10th–12th March 2026

Baton Rouge, Louisiana

www.ciprna-expo.com

Co-Hosted & Supported by::

International Association of CIP Professionals

INFRAGARD MEMBERS ALLIANCE LOUISIANA

As threats to critical infrastructure grow in scale, complexity, and frequency, the need for collaboration across government, industry, and technology has never been greater. Critical Infrastructure Protection & Resilience North America (CIPRNA) returns to Baton Rouge, Louisiana on 10th–12th March 2026, bringing together senior leaders, operators, policymakers, and solution providers to strengthen the resilience of the systems that underpin modern society.

This three-day conference and exhibition is designed to educate, connect, and equip attendees with practical strategies to protect essential assets across energy, water, transportation, communications, healthcare, and government.

In 2024, the government adopted a new foundational policy, National Security Memorandum on Critical Infrastructure Security and Resilience (NSM-22), which replaced the previous framework established by Presidential Policy Directive 21 (PPD-21). Under NSM-22, federal departments and agencies — acting as Sector Risk Management Agencies (SRMAs) — are assigned responsibility for managing risk in each of the 16 sectors. The memorandum elevates the role of Cybersecurity and Infrastructure Security Agency (CISA) as the national coordinator for critical-infrastructure security and resilience.

NSM-22 emphasizes the importance of establishing minimum security and resilience requirements for critical infrastructure entities. It calls for effective accountability mechanisms, which may include the use of regulation, federal procurement standards, grants, and financial incentives, to encourage owners and operators to meet or exceed these baseline security standards.

Under NSM-22, federal roles include coordinating cross-sector risk management; enhancing real-time information and intelligence sharing; and promoting investments in technologies and practices that strengthen resilience against evolving threats — from cyberattacks to natural hazards and supply-chain disruptions.

Since the return of the Trump administration in 2025, cybersecurity policy has been reshaped again. In June 2025, a new executive order, Sustaining Select Efforts To Strengthen the Nation's Cybersecurity (EO 14306), amended prior cybersecurity orders and re-emphasized protections for digital infrastructure, cyber resilience, and secure software development. The new order tasks federal agencies — including CISA — with accelerating adoption of stronger security practices, post-quantum cryptography, and modern secure-software development standards.

The 2025 order underlines the need to defend against nation-state cyber threats (notably from countries such as China, Russia, Iran, and North Korea) targeting U.S. systems — including those tied to critical infrastructure. It directs federal departments to harden network security, improve software supply-chain resiliency, and update standards for procurement and operations.

In this updated context, U.S. policy reflects a hybrid approach that combines the structural risk-management framework under NSM-22 with renewed, more technical cybersecurity directives under the new Trump-era order, seeking to defend critical infrastructure against both digital and physical threats in a rapidly evolving threat environment.

CIPR North America delivers a comprehensive look at both physical and cyber resilience, focusing on prevention, preparedness, response, and recovery. Attendees can expect in-depth discussion on safeguarding assets against natural disasters, cyberattacks, insider threats, terrorism, and system failures, while ensuring continuity of operations and public trust.

The event blends strategic insight with operational reality, offering case studies, frameworks, and lessons learned from real-world incidents across North America and beyond.

Conference Programme Highlights

The conference programme features keynote presentations, expert panels, and focused technical sessions led by senior decision-makers and practitioners. Across three days, the agenda is structured to support both high-level strategy and hands-on application, including:

- Executive keynotes from infrastructure owners, regulators, and national security leaders
- Sector-specific sessions addressing unique challenges in energy, water, transport, and public services
- Interactive panels encouraging cross-sector collaboration and debate
- Case studies showcasing successful resilience planning and incident response

Dedicated networking breaks and roundtables ensure meaningful engagement between speakers and delegates.

Exhibition Showcase

Alongside the conference, the CIPR North America exhibition provides a hands-on opportunity to explore the latest technologies and services supporting infrastructure protection and resilience.

The exhibition floor will feature solutions including:

- Cybersecurity platforms and OT protection
- hysical security systems and surveillance
- Risk assessment, modeling, and analytics tools
- Emergency response and communications technologies
- Asset monitoring, resilience planning, and recovery solutions

Live demonstrations and direct access to solution providers make the exhibition a valuable space for discovering innovations and building partnerships.

By attending Critical Infrastructure Protection & Resilience North America 2026, you will:

- Gain actionable insights to strengthen resilience across your organization
- Learn from real-world experiences shared by industry leaders
- Stay ahead of regulatory and threat developments
- Connect with peers facing similar challenges across sectors
- Evaluate cutting-edge technologies in one place
- Build relationships that support long-term collaboration

Whether you are responsible for security, risk, operations, IT, emergency management, or policy, CIPR North America provides the knowledge and connections needed to protect critical infrastructure in an increasingly uncertain world.

You can view the leading conference program, schedule of events, stellar speaker line up and exhibition showcase in the Preliminary Conference Programme guide available at **www.ciprna-expo.com/guide**

Join the conversation in Baton Rouge this March and be part of shaping a safer, more resilient future for North America's critical infrastructure. Register online at **www.ciprna-expo.com/register**.

Global Cybersecurity Partner:

eset Cybersecurity Progress. Protected.

Supporting Organisations:

INFRAGARD MEMBERS ALLIANCE HOUSTON · AUTO-ISAC · TRI · GBRIA · MARINE SAFE BTI · CAMO · IACI · IT ISAC · Food Ag ISAC

critical infrastructure PROTECTION AND RESILIENCE N. AMERICA

March 10th-12th, 2026

Crowne Plaza
BATON ROUGE, LOUISIANA, USA

A Homeland Security Event

Securing the Inter-Connected Society

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 10th,2026

SPECIAL RATES FOR GOVERNMENT AND OWNER/OPERATORS
Register by February 10th
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

Global Cybersecurity Partner:

eset Cybersecurity Progress. Protected.

Media Partner:

critical infrastructure PROTECTION AND RESILIENCE NEWS

Leading the debate for securing America's critical infrastructure

Supporting Organisations:

INFRAGARD HOUSTON · AUTO-ISAC · GBRIA · MARINE ISAC · CAMO · IACI · IT ISAC · Food Ag ISAC

Welcome to the 8th 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 national security, economic security, public health, or safety.

In 2024, the government adopted a new foundational policy, National Security Memorandum on Critical Infrastructure Security and Resilience (NSM-22), which replaced the previous framework established by Presidential Policy Directive 21 (PPD-21). Under NSM-22, federal departments and agencies — acting as Sector Risk Management Agencies (SRMAs) — are assigned responsibility for managing risk in each of the 16 sectors. The memorandum elevates the role of Cybersecurity and Infrastructure Security Agency (CISA) as the national coordinator for critical-infrastructure security and resilience.

NSM-22 emphasizes the importance of establishing minimum security and resilience requirements for critical infrastructure entities. It calls for effective accountability mechanisms, which may include the use of regulation, federal procurement standards, grants, and financial incentives, to encourage owners and operators to meet or exceed these baseline security standards.

Under NSM-22, federal roles include coordinating cross-sector risk management; enhancing real-time information and intelligence sharing; and promoting investments in technologies and practices that strengthen resilience against evolving threats — from cyberattacks to natural hazards and supply-chain disruptions.

Since the return of the Trump administration in 2025, cybersecurity policy has been reshaped again. In June 2025, a new executive order, Sustaining Select Efforts To Strengthen the Nation's Cybersecurity (EO 14306), amended prior cybersecurity orders and re-emphasized protections for digital infrastructure, cyber resilience, and secure software development. The new order tasks federal agencies — including CISA — with accelerating adoption of stronger security practices, post-quantum cryptography, and modern secure-software development standards.

The 2025 order underlines the need to defend against nation-state cyber threats (notably from countries such as China, Russia, Iran, and North Korea) targeting U.S. systems — including those tied to critical infrastructure. It directs federal departments to harden network security, improve software supply-chain resiliency, and update standards for procurement and operations.

In this updated context, U.S. policy reflects a hybrid approach that combines the structural risk-management framework under NSM-22 with renewed, more technical cybersecurity directives under the new Trump-era order, seeking to defend critical infrastructure against both digital and physical threats in a rapidly evolving threat environment.

We must be prepared

We must remain vigilant. The nation's critical infrastructure underpins everyday life — in energy, communications, water, healthcare, transportation, and more — and defending it requires coordinated, updated, and adaptive efforts across government, private sector, and civil society.

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

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

We look forward to welcoming you to Critical Infrastructure Protection & Resilience North America and the Crowne Plaza Executive Hotel, Baton Rouge, LA on March 10th-12th, 2026.

Register online at www.ciprna-expo.com.

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 (CIPRNA) conference in Baton Rouge, Louisiana for what will be 3 days of exciting and informative presentations and discussions on securing North America's critical infrastructure and information.

This is our 8th annual conference here in the United States and follows on from our very successful European event which took place in Brindisi, Italy in October 2025. This year we are delighted to have InfraGard Louisiana as our Co-Hosts and also the support of a number of organisations, which include, The Resiliency Initiative, Auto-ISAC, MarineSafe811, InfraGard Houston and the Coastal and Marine Operators Pipeline Industry Initiative (CAMO Initiative).

There is an exciting line up of topics and expert speakers, as you will see from the very packed agenda, where we will seek to explore the complexities and innovations in place around the protection and resilience of our Critical National Infrastructure and Information.

CIPRNA seeks to bring together leading stakeholders from industry, operators, agencies, academia and government to provide detailed insights into current policy and practices and to collaborate on the efforts required to continually address the range of challenges faced across our critical sectors.

Those challenges are exacerbated by the complexity and interconnected nature of today's global risk landscape and create ever increasing concerns for those within the infrastructure community. Threats and hazards increasingly occur together, they cascade across systems, and amplify one another.

Our societies are facing multiple threats and hazards that are unpredictable, that are new to us and have consequences that may be much broader and deeper than we might imagine.

Geopolitical tensions, climate change, system failures and human error can all lead to the disruption or failure of critical processes which can have major consequences for the functioning of our society.

Those critical processes can be disrupted by deliberate threats emanating from state actors, terrorism, activism and criminal activities. In particular, as we all know, state actors pose an increasing threat to critical infrastructure and information. This threat is apparent in, among other things, an increase in the use of hybrid tools, such as sabotage, espionage, disinformation and of course cyberattacks.

As automation grows at a pace and as the world increasingly relies on interconnected digital systems, the vulnerability of critical infrastructure to cyber risks continue as a pressing concern.

In our endeavours to deal with the range of challenges, across both the physical and cyber spectrums and alongside the increasing scale of natural events and disasters, we have to continually consider our approach to the protection and resilience of our critical entities.

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

The conference is specifically designed to stimulate debate and your active participation across the sessions will add real value in the development of new thinking. I know you will find this a most rewarding and enjoyable event and I look forward to seeing you in Baton Rouge.

John Donlon QPM FSyl
Conference Chair

Follow us:

Critical Infrastructure Protection & Resilience

Why Attend?

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

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

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

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

For conference or registration queries please contact:
Ben Lane
Event Director
E: benl@torchmarketing.co.uk

Who Should Attend

Critical Infrastructure Protection and Resilience North America is for:

- Local/State/Federal 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/State 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, Louisiana 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."

Exhibition Opening Hours		On-Site Registration Hours	
Tuesday March 10th	1.00pm to 7.30pm	Tuesday March 10th	8.00am to 6.00pm
Wednesday March 11th	9.00am to 5.30pm	Wednesday March 11th	8.30am to 5.00pm
Thursday March 12th	9.00am to 4.30pm	Thursday March 12th	8.30am to 4.00pm

REGISTER ONLINE AT WWW.CIPRNA-EXPO.COM

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

REGISTRATION

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

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

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

EARLY BIRD DISCOUNT - deadline February 10th, 2026

Register yourself and your colleagues as conference delegates by February 10th, 2026 and save with the Early Bird Discount. Registration details can be found at www.ciprna-expo.com/register.

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

Discounts for Members of Supporting Associations

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

- INFRAGARD Louisiana and INFRAGARD Houston
- National Security & Resilience Consortium (NS&RC)
- International Association of CIP Professionals (IACIPP)
- International Security Industry Organization (ISIO)
- International Association of Certified ISAOs (IACI)
- Auto ISAC

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

Schedule of Events

Tuesday March 10th, 2026

1:00pm - Exhibition Opens

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

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

4.00pm-5:30pm - Session 1: National & Regional Emergency Management Preparedness

5:30pm - Networking Reception in Exhibition Hall

Wednesday March 11th, 2026

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: Cybersecurity Regulations, Best Practice and Minimum Standards

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

2:00pm-3:30pm - Session 4a: Cyber Threats, Cybersecurity and AI in CI

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

4:15pm - 5:30pm - Session 5a: Risk Management & Mitigation Strategies

Track Two

9:00am-10:30am - Session 2b: Communications Sector Symposium

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: Power & Energy Sector Symposium

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

4:15pm - 5:30pm - Session 5b: Maritime, Ports and Pipelines Symposium

Thursday March 12th, 2026

9:00am-10:30am - Session 6a: Strategic Resilience Planning

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

11:15am - 12:30pm - Session 7a: Drones and UAS

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

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

11:15am - 12:30pm - Session 7b: Secure by Design

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

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

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

4.30pm - Exhibition Close

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

Tuesday March 10th

Conference Programme

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

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

Madhu.Gottumukkala, Acting Executive Director, Cybersecurity and Infrastructure Security Agency (CISA)*

Clay Rives, Director, Mayor's Office of Homeland Security and Emergency Preparedness

Col. Robert Hodges, Deputy Secretary of Public Safety Services, Louisiana State Police

Brian Harrell, Former Assistant Secretary for Infrastructure Protection

Lester Millet III, President, Infragard Louisiana

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

4:00pm-5:30pm - Session 1: National & Regional Emergency Management Preparedness

Comprehensive efforts need to be undertaken by governmental bodies, operators, private sector entities, and other stakeholders, at both national and regional levels to anticipate, prevent, prepare for, respond to, and recover from incidents that could disrupt the functioning of critical infrastructure systems. From risk assessment and identification of potential threats and hazards, to understanding the vulnerabilities of these systems, and the complex interdependencies and cascading failures among different critical infrastructure sectors, developing comprehensive emergency strategies to mitigate them is key to successful resilience.

Chair: John Donlon QPM, FSyI

Joe Threat, Chief Resilience Officer and Deputy Chief Administrative Officer for Infrastructure, City of New Orleans

The Challenges of Critical Infrastructure Protection: Lessons of Ukraine - Oleksandr Sukhodolia, Leading Consultant of Critical Infrastructure Protection Department, The State Service of Special Communications and Information Protection of Ukraine

Preparing Emergency Management/Responder Facilities to Continue Providing Essential Functions During a Long-Duration, Widespread Power Outage - Michael Lambert, Emergency Preparedness/Homeland Security Planner, Houston-Galveston Area Council of Governments

Incident Stories From Peak Season: City Grids and Factory Lines Under Fire - Charles Everette, Chief Information Security Officer, City of Fort Lauderdale

Charting An Alternate Path to Achieving State and Local Preparedness - Ollie Gagnon, Chief Homeland Security Advisor, Idaho National Laboratory

---

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

**invited*

Wednesday March 11th

Track One

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

This session investigates the evolving landscape of threats against CI, which include terrorism, insider threats, climate and cyberattacks including the emerging challenges asserted by AI, which necessitate a proactive approach to security. To effectively address these emerging challenges, it is crucial to identify, monitor, and assess their potential impact.

***Chair:** John Donlon, IACIPP*

Senior Representative, FBI*

Mark Fontenot, ICC Manager, Governor's Office of Homeland Security and Emergency Preparedness

Senior Representative, Cybersecurity & Infrastructure Security Agency*

Cybersecurity - Global Trends 2026 - Jean-Ian Boutin, Director of Threat Research, ESET

TBC

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

11:15am-12:30pm - Session 3a: Cybersecurity Regulations, Best Practice and Minimum Standards

The threat of cyber-attacks by state actors and hacktivists continues to grow as a threat to cause disruption to our infrastructures. We are behind the curve against the attackers, so developing legal requirements, recommended and best practices, and foundational security controls is important to ensure operators and agencies are meeting expected regulation requirements to prevent a successful attack, or what to do following a cyber breach.

***Chair:** Mike Echols, Max Cybersecurity*

Senior Representative, Cybersecurity & Infrastructure Security Agency*

Critical Infrastructure Sector implementation of the Cybersecurity Framework - Ron Martin, Professor of Practice, Capitol Technology University

Engineering against Digital Risk in CIP Applications: Cyber-Informed Engineering Use Cases - Benjamin Lampe, Instrumentation and Control Engineer, Idaho National Laboratory

Senior Representative, IT-ISAC*

Deborah Kobza, President, IACI

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

Track Two

9:00am-10:30am - Session 2b: 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 critical for businesses, government and all sectors of CI.

From Design to Deployment: Security Architecture and Operating Models in Utility Private Wireless - Anuj Kumar, Cybersecurity Manager – Enterprises, Nokia

Quality at Scale: A New Standard for Reliable, High-Performance Data Centers - Mike Regan, VP Business Performance , Telecommunications Industry Association (TIA)

Critical Communication Networks - Keeping the Channels Open - Graeme Hull, Managing Director, SWISSPHONE LLC

Enabling Critical Infrastructure Security and Operational Efficiency via Private Cellular AI enabled Telecom Open ISAC and SCADA IO processing Capability - Brenda Connor, Professor of Practice & Senior Technical Managing Director, Texas Tech University Critical Infrastructure Security Institute

Incommunicado Island: 18 years of incomplete interoperable communications - Jeffrey Quinones-Diaz, Consultant, The Consulting Lead 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.

Adam Stahl, Senior Advisor, TSA*

Janet St. John, Director of Cybersecurity, AAR

Faye Francy, Executive Director, Auto-ISAC

Chris Engelbrecht contact, MO DOT / AASHTO*

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

Wednesday March 11th

Track One

2:00pm-3:30pm - Session 4a: Cyber Threats, Cybersecurity and AI in CI

The cyber threats to Critical Infrastructure continue to increase at the reward of financial gain or major disruption, where chinks in the armour continue to be exposed by malicious actors. How do we better protect the confidentiality, integrity, and availability of IT and OT systems. What role can AI play in assisting cybersecurity processes?

Joshua Tannehill, Interim Commander, Cyber Reserve Team, Louisiana State Guard; President Louisiana Chapter, Cloud Security Alliance; VP Louisiana Chapter, InfraGard LA

Cybersecurity for Water in an Age of Advanced Persistent Threats - Ymir Vigfusson, CTO, Keystrike

From Digitalisation to Intelligent Resilience: How AI Is Transforming Cybersecurity and Safety in Critical Infrastructures - Jalal Bouhdada, CEO, Indurex, Netherlands

The Sovereign Stack: A New Doctrine for Coordinated Critical Infrastructure Defense Against Nation-State Actors - Bradley Tenenholtz, Product Security Officer, Becton Dickinson

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

4:15pm-5:30pm - Session 5a: Risk Management & Mitigation Strategies

Risk management and mitigation strategies in critical infrastructure are essential for ensuring uninterrupted essential services. With the nation hosting the 2026 World Cup, this process includes identifying, assessing, and treating risks to vital assets, systems, and networks, as well as large event venues and other crowded places. These high-visibility locations require strengthened protective measures to safeguard attendees and support the resilience of infrastructure operations during this period of increased global attention and significantly elevated activity.

Sustaining PNT Systems Beyond A 30-Day GPS Disruption - Mike Roskind, PNT Program Manager, CISA/NRMC/Space Systems & Services

Leveraging Technology for Predictive Infrastructure Planning and Resilience in Critical Infrastructure (CI) Systems - Robert Stephan, Specialist Executive, Deloitte

Model Based Systems Engineering (MBSE) Analysis & Update of U.S. Infrastructure Data Taxonomy (IDT) Using U.S. National Critical Functions (NCFs) - Anthony Adebonojo, Chairman, Critical Infrastructure (CIPR) Working Group, International Council of Systems Engineers

Mike Jackson, President, Elite Edge

Track Two

2:00pm-3:30pm - Session 4b: Power & Energy Sector (Grid Resilience) 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, and build greater grid resilience?

Tommy Waller, President & CEO, Center for Security Policy

Impact of equipment mechanical vulnerabilities on the electrical grid: A study of seismic vulnerabilities in transformer bushings - Chandrakanth Bolisetti, Senior Research Scientist, Idaho National Laboratory

TBC

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

4:15pm-5:30pm - Session 5b: Maritime, Ports and Pipelines Symposium

The maritime, ports and pipelines sectors are vital for global trade and energy security. Protecting these systems from physical and cyber threats prevents economic disruption, environmental disasters, and ensures the continuous flow of goods and resources essential for national security and prosperity.

Mel Carraway, Region 4 Security Director, TSA*

Securing ONG, Chemicals, and Maritime Critical Infrastructure: Enhancing Resilience in Industrial Control Systems - Marco Ayala, President, InfraGard Houston

Ed Landgraf, Chairman, Coastal And Marine Operators

Maggie O'Connell, Director of Security, Reliability, and Resilience, Interstate Natural Gas Association of America (INGAA)

Thursday March 12th

Track One

9:00am-10:30am - Session 6a: Strategic Resilience Planning

A holistic, long-term approach towards building resilience is required to ensuring the continued functioning of CI, especially when faced with increasing frequency and severity of disruptions. It moves beyond traditional "disaster recovery" to embrace the ability to anticipate, adapt, and transform in the face of a wider range of evolving and interconnected threats, embedding resilience thinking into the core values, policies, and daily operations of critical infrastructure organizations and government bodies.

Synergising Critical Infrastructure Protection, Resilience, Cybersecurity and Continuity of Operations to Achieve and Sustain Critical Infrastructure Preparedness – Jeff Gaynor, President, American Resilience

Andrea Davis, President & CEO, The Resiliency Initiative

Stakeholder Information Protection and Sharing – Chris Miller, PCII Program Office Outreach Leader, Cybersecurity & Infrastructure Security Agency

Building Resilience in Critical Infrastructure - Glenda Snodgrass, President, The Net Effect, LLC

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

11:15am-12:30pm - Session 7a: Drones and UAS

Drones pose a growing threat to critical infrastructure due to their increasing accessibility, manoeuvrability, and payload capacity. They can be used for surveillance, delivering explosives, or causing disruptions. However, drones can also act as a facilitator to protect critical infrastructure. In this session we look into the threat, counter measures and impact drones can induce on CI.

George Rey, Sector Chief Program - COTS Technology, Infragard LA

Adapting to Aerial Threats: Scalable Non-Disruptive, Non-Kinetic Counter-UAS Strategies for Critical Infrastructure Resilience - Danny Rajan, GM USA, D-Fend Solutions

Charles Dick, Airsight*

TBC

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

Track Two

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

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

Charles Everett, Field CISO Advisor, ESET

Detecting the undetectable: overcoming clutter, weather, darkness, and occlusion - Curtis Walters, VP of Sales - Commercial, Echodyne

TBC

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

11:15am-12:30pm - Session 7b: Secure by Design

Secure by Design is about embedding security as a non-negotiable quality attribute throughout the entire lifecycle of critical infrastructure, making it inherently more robust, resistant to attack, and capable of recovering quickly from inevitable disruptions. From Threat Modeling and Risk Assessment to Secure Supply Chain, it's making security a foundational characteristic from the initial concept and design phase, through development, deployment, operation, and eventual decommissioning.

Importance of Embedding a Holistic Approach to Security and Resilience in the Design of Airport Infrastructure - Sarah-Jane Prew, Associate Aviation Security Consultant, Arup UK

Transforming Landscapes. How UK CT policing is supporting Aviation Security - DS Kirsty Rigg, Counter Weapons Threat Team Lead, National Counter Terrorism Security Office UK

Embedding Enterprise Cyber Resilience into Critical Infrastructure - Charles Burton, Information Technology Director, Calcasieu Parish Police Jury

A Holistic Approach to Securing Critical Infrastructure: Beyond Technology and Tactics - Ric Everett, Senior Security Consultant, IMEG

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

Thursday March 12th

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

Information sharing and cooperation is crucial for effective risk management and resilience planning. By fostering collaboration among government, operators, and communities, we can enhance the protection of critical infrastructure. However, barriers to information sharing and cooperation persist, partly due to trust. To overcome these challenges, we must build trust and create a supportive environment that encourages open communication and knowledge exchange.

Chair: John Donlon QPM FSyI

Navigating CISA: Programs, Services, and Building Strategic Partnerships - Samuel M. Duchac, Executive Officer, Regional Sector Outreach Coordinator, Regional Training & Exercises Coordinator, Cybersecurity & Infrastructure Security Agency

Lester Millet, President, Infragard LA

What can the National Weather Service (NWS) do for you? - Lauren Chandler, Warning Coordination Meteorologist, National Weather Service

Public Private Partnerships to Increase Community Preparedness- how the CAER group trains and exercises with local emergency management and hazmat teams - Josie Ross, Emergency Management Officer, City of Henderson

Senior Representative, National Council of ISACs

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

Networking Reception

Tuesday March 10th
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

Crown Plaza Baton Rouge
4728 Constitution Ave
Baton Rouge
LA 70808

Located in the heart of Baton Rouge, just off I-10 and College Drive, Crowne Plaza Executive Center Baton Rouge is 10 minutes from the LSU campus and a short drive from Baton Rouge Metropolitan Airport (BTR). Near top attractions like Downtown Baton Rouge, the Louisiana State Capitol, BREC's Baton Rouge Zoo, the LSU Rural Life Museum, and the Mall of Louisiana, we are the ideal choice for your Baton Rouge adventure.

Host meetings and events in our 18 venues within 32,000 square feet of space. Savor Louisiana flavors at our restaurants. Take a dip in our outdoor pool and stay active in our expansive fitness center. Our pet-friendly, spacious accommodations offer free Wi-Fi with plush bedding to sink into at the end of the day. We are your gateway to the best of Baton Rouge!

For more details on the hotel and online booking visit **www.ciprna-expo.com/accommodation**

Booking Your Accommodation

Special Room Rate for CIPRNA Delegates – $163 prpn (excl taxes)

Promo Code: '**CIP**'

Book your hotel accommodation at the **Crown Plaza Baton Rouge** 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

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

Special Group Rate ends 17th February

We look forward to welcoming you to Baton Rouge, LA.

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:

Bruce Bassin
Americas
E: bruce@torchmarketing.co.uk
T: +1 702.600.4651

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

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 - $19,500
- Gold Sponsor - $15,500
- SIlver Sponsor - $10,950
- Bronze Sponsor - $8,950
- Conference Proceedings Sponsor - $5,950
- Delegate Folder Sponsor - $4,950
- Networking Reception Sponsor - $4,950
- Coffee Break Sponsor - $4,950
- Site Visit & Coach Sponsor - $4,950
- Lanyard Sponsor - $4,950
- Badge Sponsor - $4,950

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' - $3,495
Table Top Exhibit 10'x10' - $5,495
Raw space with 1 x table and 2 x chairs, pipe and drape, electrical socket, wi-fi, 1 Exhibitor Delegate pass (2 for 10x10 booth) with full conference access, lunch and coffee breaks included, listing in the official event guide and website.

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

ASK ABOUT OUR BOOKING BUNDLES FOR EXTRA EXPOSURE

ALL PRICES SUBJECT TO 10.5% BR/LA SALES TAX

Sponsors and Supporters:

We wish to thank the following organisations for their support and contribution to Critical Infrastructure Protection & Resilience North America 2026.

Global Cybersecurity Partner:

ESET Cybersecurity Progress. Protected.

Supported & Co-Hosted by:

International Association of CIP Professionals

INFRAGARD MEMBERS ALLIANCE LOUISIANA

Bronze Sponsor:

ECHODYNE

Badge & Coffee Break Sponsor:

AXIS COMMUNICATIONS

Lanyard Sponsor:

CAPITOL Technology University

Supporting Organisations:

INFRAGARD MEMBERS ALLIANCE HOUSTON

AUTO-ISAC

IT ISAC

Food Ag ISAC

IACI

GBRIA

CAMO

NS&RC

ISIO

Help2Protect

Flagship Media Partner:

critical infrastructure PROTECTION AND RESILIENCE NEWS

Media Supporters:

govCIO OUTLOOK

BIOMETRIC

BORDER SECURITY REPORT

CIO Review

Owned & Organised by:

TORCH

Participating Organizations Have Included:

Highlighted Speakers

Brian Harrell

Former Assistant Secretary for Infrastructure Protection, DHS

Brian currently serves as the Vice President and Chief Security Officer (CSO) for a large energy company with assets and operations in 25 states. He is responsible for the company's physical and cybersecurity, privacy, intelligence, and business continuity units.

In 2018, Brian was appointed by the President of the United States to serve as the sixth Assistant Secretary for Infrastructure Protection, at the Department of Homeland Security. Brian also served as the first Executive Assistant Director for Infrastructure Security at the U.S. Cybersecurity and Infrastructure Security Agency (CISA).

Brian has spent time during his career in the US Marine Corps and various private sector agencies with the goal of protecting the United States from security threats.

Oleksandr Sukhodolia

Leading Consultant of Critical Infrastructure Protection Department, The State Service of Special Communications and Information Protection of Ukraine

Oleksandr Sukhodolia works at the National Institute for Strategic Studies of Ukraine and takes position of a Head of Critical Infrastructure Protection, Energy and Ecological Security Department. He is also Leading Consultant of Critical Infrastructure Protection Department, The State Service of Special Communications and Information Protection of Ukraine.

Oleksandr Sukhodolia has extensive experience in public service and higher education. Since 1998, he has been working on issues of energy security at different positions at governmental agencies. Currently his research interests focused on the energy security, critical infrastructure security and resilience. Oleksandr has led the development of the Law of Ukraine "On Critical Infrastructure" (2021) and later contributed to drafting the regulatory acts to implement provision of the Law. O.Sukhodolia co-authored the books, namely: "Developing the critical infrastructure protection system in Ukraine" (2017), "Organizational and legal aspects of ensuring the security and resilience of Ukraine's critical infrastructure" (2019), "Energy Security of Ukraine: Methodology of System Analysis and Strategic Planning" (2021). Oleksandr holds a Ph.D degree in Electrical Engineering and Dr. (Habil) in Public Administration.

Tommy Waller

President & CEO, Center for Security Policy

Lt. Col. Tommy Waller, USMC Ret is the President and CEO of the nonprofit Center for Security Policy. Waller retired from the Marine Corps Reserves at the rank of Lieutenant Colonel after serving more than two decades on both active duty and in the reserves with deployments to Afghanistan, Iraq, Africa, and the Caribbean. His last military assignment was as the Commander of the Marine Corps Reserve's only Force Reconnaissance Company. While in the Corps, he graduated from the Marine Corps Command and Staff College and was cross assigned to serve as a key staff member of the U.S. Air Force's Electromagnetic Defense Task Force (EDTF). During his decade of civilian service to the Center for Security Policy he has led the nationwide "Secure the Grid Coalition," helping inspire policies to secure this most critical infrastructure at the federal, state, and local levels. Waller holds a BA in International Relations from Tulane University, New Orleans, LA and was the first recipient of the Captain Robert M. Secher Scholarship to the Wharton School of Business where he completed an executive education course on high stakes negotiations.

Euclid Talley

Assistant Director, Governor's Office of Homeland Security and Emergency Preparedness (GOHSEP)

Euclid Talley's current assignment is as Assistant Director for Security and Interoperability, working for the Governor's Office of Homeland Security and Emergency Preparedness, managing critical infrastructure protection, cyber security, criminal intelligence, emergency communications, and the Louisiana Center for Safe Schools. He provides oversight for vulnerability threat assessments and security protection planning to critical infrastructure of national interest e.g. national defense, national security, or national resource protection. Additional areas of responsibility include Overseeing and safeguarding information, personnel, property, assets, and/or material from theft, loss, misuse, fraud, disclosure, espionage, sabotage, or terrorism.

He has four years of military service managing Human Resources, Officer Recruiting, and Career Management for a force of 9,000+ Soldiers, including medical doctors, dentists, lawyers, and mental health providers, along with basic combat and combat support branches.

Euclid also has eight years of military service assigned as the WMD Consequence Manager, responding to emergency incidents and providing direct support to Federal/State and civilian authorities conducting counter-terrorism to CBRNE events. Areas of responsibility included providing identification, mitigation, lab analysis, evidence preservation, intelligence analysis, physical security to special events, and force protection. He handled all natural and manmade Disaster Recovery projects and provided POTUS Protection in support of the Secret Service Hazardous Materials Mitigation Unit during multiple events.

He also has ten years of military assignments assigned as the Construction Project Management and Engineering Operations Program Management for critical infrastructure rebuild and force protection projects in support of Operation Freedom's Sentinel- Afghanistan and Operation Iraqi Freedom. Assigned as Construction Project Management for projects valued over $28M. Managed Natural Disaster Recovery and Force Protection Engineer Construction projects, e.g., Honduras, Belize, Norway, and CONUS, in support of civilian and military authority.

Lester Millett III

InfraGard Louisiana President And Port Of South Louisiana Safety Risk Agency Manager

InfraGard Louisiana President and Port of South Louisiana Safety Risk Agency Manager Lester Millet III was recently awarded the 2020 Government Technology & Services Coalition Homeland Security Today Citizen of Mission Award. The award goes to an individual who devotes personal time, energy and resources to work for causes related to homeland security. Volunteers, nonprofit leaders, corporate employees and others are eligible for nomination as long as they devote time and effort to supporting the homeland mission.

Anuj Kumar

Senior Security Architect, Nokia

Anuj Kumar is a distinguished technology executive with over 15 years of experience in the telecommunications industry. He specializes in empowering Communication Service Providers (CSPs) globally to securely design, optimize, and scale their core network infrastructures and business operations systems. His expertise encompasses a broad spectrum of critical telecom domains, including:

• 5G Service-Based Architecture; • 4G-LTE; • IMS VoLTE; • Subscriber Data Management (SDM); • Online Charging Systems (OCS); • Policy Management (PCRF); • Broadband and Fiber Operations; • 5G/ Private 5G Monetization

Before joining Nokia, Anuj Kumar held several key leadership positions in the telecom and IT sectors. Notably, he served as a Core Solution Consultant at Salesforce, where he spearheaded 5G Monetization and BSS transformation initiatives for telecommunications customers across North America, driving transformation in their sales and support channels.

Benjamin Lampe

Engineer, Idaho National Laboratory

Mr. Benjamin Lampe is an Engineer and Researcher at the Idaho National Laboratory (INL), specializing in Cyber-Informed Engineering since September 2023. Previously, I held a position as a faculty member in the ICS Cybersecurity program at Idaho State University, where I was a Joint Appointee with the INL. My professional journey includes significant roles at the Naval Nuclear Laboratory (NNL), where I served as an Operational Technology (OT) Enterprise Architect, Systems Analyst, and a Controls Engineer. In these roles, I formulated the OT technical strategy and implemented a nation-wide OT infrastructure between the NNL's process systems. As a Control Engineer, I maintained a myriad of process and monitoring systems within power distribution, water and wastewater management, building automation, and radiological monitoring. I have a Bachelor of Science in Electrical Engineering from the University of Wyoming, and a Master of Science in Computer Science from the University of Idaho.

Joshua Tannehill

Information Systems Security Officer | VP Louisiana Chapter, Knight Federal Solutions | InfraGard

Knight Federal Solutions – Information Systems Security Officer
Support US Army at JRTC at Fort Polk to protect their classified network

Global Data Systems – Cybersecurity Sales Engineer
Support our sales teams as a cybersecurity subject matter expert in a sales analyst and sales engineering type of consultancy role.

Lumen Technologies – Senior Manager, InfoSec
People manager of a 9 person Trust & Safety team that supported Law Enforcement Support requests and kept the internet clean from cybercrime and abuse.

US Air Force and Air National Guard
Iraq war veteran and Protected the US Air Force from cyber-attacks and was the equivalent of the Chief Cybersecurity Compliance Officer for the Louisiana Air Force National Guard upon retirement in 2019.

John Donlon

Chairman, International Association Of CIP Professionals

John Donlon joined the police service in 1976 where he served in a wide variety of roles including; operational policing, major crime investigation, training and specialist operations. He was an accredited Gold Commander for Firearms, Public Order and Major Sporting Events. He was also a qualified Senior Investigating Officer.

In July 2005, as a Chief Officer, John was appointed to a National role within the world of Counter Terrorism and National Security, working with the Association of Chief Police Officers, Metropolitan Police (New Scotland Yard) and the UK Government. It was here that he provided the strategic policing lead on all matters within the Protect and Prepare portfolio of the UK Counter Terrorism Strategy, CONTEST.

Within his Protect remit he was accountable for the oversight of Special Branch and protective security policing at ports-encompassing all modes of transport, the National Counter Terrorism Security Office (NaCTSO) and the police contribution to protecting Crowded Places and the UK Critical National Infrastructure.

For Prepare, he had responsibility for the national police response to effectively manage a range of terrorist attacks, as outlined in the National Risk Assessment, building resilience, the national Counter Terrorism training portfolio and incorporating learning from CT incidents and exercises.

Anthony Adebonojo

Chairman, Critical Infrastructure, Protection & Recovery Working Group (CIPR-WG), International Council of Systems Engineers (INCOSE), USA

Mr. Adebonojo works for Northrup Grumman Corporation as a Senior Staff Systems Engineer on a National Security Program, however he is speaking in his role as the Chairman of the INCOSE Critical Infrastructure Working Group (INCOSE CIPR-WG) at this event. INCOSE is the Premier organization involved in the promotion of Systems Engineering world-wide. It consists of 52 Working Groups and Mr. Adebonojo is the Chairman of the Critical Infrastructure Working Group. He has been involved in the modelling of Critical Infrastructure Systems as part of this Working Group for over four Years.

In his current role, he is responsible for teaching younger engineers how to model system interfaces (or interdependencies) for a major Weapon Systems for Northrup Grumann. He has also held roles as an Enterprise Architect and Verification and Validation Engineer for DoD Weapon Systems as well.

Mr. Adebonojo has been involved in Systems Engineering and architecture for over 21 Years and is an INCOSE Certified Systems Engineering Professional (CSEP) as well as a Certified Information Systems Security Professional (CISSP) and a OMG-Certified Systems Modelling Professional (OCSMP L2).

Charles Burton,
Technology Director, Calcasieu Parish Government

Charles Burton has led technology teams in Louisiana government for 20 years and is currently the Calcasieu Parish Technology Director. Data Center and communication modernization projects along with Cybersecurity programs have been some of his successful accomplishments with disaster recovery being one of the more challenging success stories. He holds a Masters in Cybersecurity and bachelor's in computer science. His certificates include ITIL, PMP, CGCIO, CISSP, CompTIA as well as Microsoft certificates.

Mr. Burton serves on several boards and committees at the State and Local level, he speaks at conferences and advises on the topics of Cybersecurity & Technology. Mr. Burton is involved in several community organizations where he resides in Lake Charles, LA with his wife and family.

Lauren Nash

Warning Coordination Meteorologist, National Weather Service,

Lauren Nash has been the Warning Coordination Meteorologist at NWS New Orleans/Baton Rouge since September 2020. Her main job is to interface and interact with our local partners, making sure their needs are met and our products are well understood. She also oversees community outreach, quality control, improvements of our products and overall ensuring we are a great partner in our community. Previously, she worked in Tallahassee, FL, Huntsville, AL, and New York City. She has a Bachelor's degree in Meteorology and a Master's Degree in Public Administration. In her free time, she enjoys relaxing with her two cats, scuba diving, traveling and enjoying all the city of New Orleans has to offer. She has an Undergraduate degree in Applied Meteorology with Minors in Aviation Operations and Airport Business from Embry-Riddle Aeronautical University. She has a Master's in Public Administration from Park University.

Dr Ron Martin, CPP, CPOI

Professor Of Practice, Critical Infrastructure, Capitol Technology University

Dr. Martin is a Professor of Practice at Capitol Technology University. His work at Capitol Technology University is in the following functional areas Critical Infrastructure, Industrial Control System Security, Identity, Credential, and Access Management. Ron has relationships with a diverse mix of businesses. He serves as a board of directors for many profit and non-profit organizations. Ron retired from the United States (U. S.) Army in 1999 and the U. S. Government in 2011. In between his Federal Service tours, he served five years as a civilian police officer in the Commonwealth of Virginia. During his Federal Service, he served with the U. S. Department of Commerce and Health and Human Services as the program director to develop and implement both department's Identity, Credentialing and Access Management (ICAM) Programs. Ron is a voting member of the United States Technical Advisory Group to the International Standards Organization (ISO), which works to develop and articulate the U.S. position by ensuring U.S stakeholders' involvement from the private and public sectors. Dr Martin serves as the North Louisiana Vice President of the InfraGard Louisiana Membership Alliance (ILMA). At ILMA he serves as the Critical Infrastructure Protection, Commercial Facilities Sector Chief. Ron holds a Ph.D. Technology, Capitol Technology University, a Master of Science in Management, Frostburg State University, Bachelor's degree in Police and Public Administration, George Mason University, and an AAS Degree in Police Science, Northern VA Community College.

Joseph Threat

Chief Resilience Officer and Chief Administrative Officer, City of New Orleans

Joseph Threat brings over four decades of distinguished expertise in crisis management, grant management, security training, executive municipal infrastructure operations/construction and emergency operations across both military and civilian sectors.

Beginning his career in the United States Marine Corps in 1968, Mr. Threat served multiple tours in Vietnam, accumulating over 26 years of service and retiring as a senior Warrant Officer. His military accolades include the Meritorious Service Medal, Navy Commendation medal with Combat "V" for Valor, and others recognizing his leadership and bravery.

Transitioning to civilian life, Mr. Threat assumed the role of Chief Executive Officer at Innovative Logistic Support Services (ILSS), where he spearheaded its growth into a multi- million-dollar business. Following this, he founded "Threat Defense," his consulting firm, providing strategic guidance until 2018. Notably, Mr. Threat served as Executive Director for FEMA's Louisiana Recovery Office, overseeing $37 billion in recovery funding post-Hurricanes Katrina, Rita, and other major disasters.

Currently serving an eight-year term as the Chief Resilience Officer and as the recently appointed Chief Administrative Officer for Infrastructure in the City of New Orleans. Mr. Threat plays a pivotal role in managing operations, emergency response, and capital projects. He has navigated numerous crises, including the Hard Rock Hotel collapse, Terrorist attacks, the COVID-19 pandemic, Super Bowl XIV and multiple hurricanes, demonstrating his steadfast leadership and commitment to public service.

Josie Ross

Emergency Management Officer, City of Henderson Department of Emergency Management

Josie Ross is the Emergency Management Officer for the City of Henderson Department of Emergency Management. Her work focuses on Continuity Planning, ICS training, exercises, hazardous materials and large scale special events. She is part of the planning team and serves as ESF 5 at the County MACC for the Superbowl, Formula 1 and New Year's Eve. She is the co-chair of the CAER group and serves on the LEPC and SERC. She has a Masters Degree in Emergency Management.

Andrea Davis

President and CEO, The Resiliency Initiative, USA

Andrea Davis is a recognized expert in the field of emergency management who has dedicated her career to bridging the silos between the public and private sectors to create a united approach when it comes to disaster risk reduction.

Ms. Davis has held leadership roles with NGOs (The American Red Cross, Save the Children US), the US Federal Government (FEMA, The Federal Reserve) and for Fortune 500 Companies (Walmart, Disney). With each role, Ms. Davis used her influence to lead global initiatives focused on the importance of making risk-informed determinations and engaging all members of the community in the decision-making process. Currently, Ms. Davis is the President and CEO of a Women Owned Small Business (WOSB), The Resiliency Initiative (TRI). Ms. Davis founded TRI out of a passion to serve the whole community before, during, and after an emergency.

Ms. Davis is a decorated leader. She was selected as the inaugural Emergency Manager of the Year by the International Association of Emergency Managers in 2018 and was inducted into the Women's Hall of Fame for Emergency Management in 2013.

Michael Lambert

Emergency Preparedness/Homeland Security Planner, Houston-Galveston Area Council of Governments

Michael Lambert is an Emergency Preparedness/Homeland Security Planner for the Houston-Galveston Area Council of Governments. Michael is an experienced emergency manager with nearly two decades working on issues related to the electric grid.

Michael has been a frequent panellist and speaker on the emergency management perspective of electric grid fragility, threats and resilience.

Among the organizations of which Michael is a member are the Secure the Grid Coalition, the Electric Infrastructure Security Council and the Texas Energy Working Group. He serves on the Texas Critical Infrastructure Protection Task Force and is an Infrastructure Liaison Officer with the State of Texas.

Dr. Brenda Connor

Senior Technical Managing Director, TTU Critical Infrastructure Security Institute, USA

Dr. Brenda Connor has a dual appointment at Texas Tech University as Professor of Practice in the Department of Electrical and Computer Engineering and as Senior Technical Managing Director for the Critical Infrastructure Security Institute (CISI). CISI's mission is to advance the protection, resilience, and security posture of our nation's critical infrastructure systems by developing cutting-edge solutions to emerging security challenges through interdisciplinary research, innovative education, and strategic partnerships. Dr Connor joined TTU in Jan 2025 after a 30-year career with Ericsson and is focused on applied research to accelerate the critical infrastructure operator's business case to deploy a private cellular network.

Her research areas include:
• Critical Infrastructure Security and Operational Efficiency via Private Cellular AI enabled Integrated Sensing and Communications (ISAC) and SCADA IO processing capability for national security with dual use relevance for DOD.
• NVIDIA based AI Model & Algorithms development and reuse.

Ed Landgraf

Chairman, CAMO Pipeline Group and Director of Texas 811 Marine Safety and Operations

Ed is the founder of CAMO "Coastal And Marine Operators" non-profit Pipeline industry group and serves as Chairman of the Board. Ed is also employed by Texas 811 as Director of Marine Safety and Operations. Ed is also the Pipeline Sector Chief of Louisiana Infraguard.

Ed has worked in the oil and gas industry for 33 years. A native of Oklahoma and graduate of Oklahoma State University, Ed's first assignments started in Texas, New Mexico, and Colorado. Ed then spent 26 years dedicated to Gulf Coast Region with special assignments in New Zealand and Australia. His roles included managing infrastructure protection, security, risks management, 811 education, marine safety processes, corporate sustainability, and many innovative initiatives. Ed is also an expert witness for marine pipeline accidents.

Ed has 17 years of volunteer service to the community as Vice- Chairman of Coastal Zone Management, Chamber of Commerce Board of Directors, member of the National Estuary Program's Management Committee, and Coastal Conservation Association Board of Directors.

Ed founded CAMO – "Coastal And Marine Operators" group in 2009. CAMO now has over 30 participating companies, NGO's and agencies, all working to enhance underwater infrastructure security, integrity, damage prevention, and public safety by designing and implementing new innovative solutions.

Marco Ayala

President, Houston InfraGard Members Alliance

Marco Ayala has 30 years of field experience where he designed, implemented, and maintained process instrumentation, automation systems, safety systems, and process control networks. In his role with large global manufacturing company, he is responsible for applications globally that are specific to plant site operations and corporate governance.

With around two decades focused specifically on industrial cybersecurity, he has led efforts to secure the oil and gas (all streams), maritime port, offshore facilities, and chemical sectors, supporting federal, local, and state entities for securing the private sector.

Marco is highly active in International Society of Automation and is a longtime member and newly elected into the Executive Board. He is a 22-year Senior Member and a certified cyber instructor for ISA (62443) with volunteering commitments and contributor to the AMSC Gulf of Mexico (GOM) cybersecurity committee in a sworn in role to the USCG as Chair of Threat Intelligence and Cybersecurity for the outer continental shelf (OCS).

InfraGard member since 2014, and currently serving as the President for the Houston Members Alliance.

Full speaker lineup at www.ciprna-expo.com/speakers

DELEGATE REGISTRATION FORM

EARLY BIRD SAVINGS

Book your delegate place by 10th February 2026 and save with the Early Bird rate

REGISTRATION IS SIMPLE

1. Register online at www.ciprna-expo.com/register
2. Complete this form and email to: ciprna@torchmarketing.co.uk
3. Complete this form and mail to: CIPRNA 2025, Torch Marketing, 200 Ware Road, Hoddesdon, Herts EN11 9EY, UK.

DELEGATE DETAILS

(Please print details clearly in English. One delegate per form, please photocopy for additional delegates.)

Title: _____ First Name: _____

Surname: _____

Job Title: _____

Company: _____

E-mail: _____

Address: _____

Street: _____

Town/City: _____

County/State: _____

Post/Zip Code: _____

Country: _____

Direct Tel: (+) _____

Mobile: (+) _____

Direct Fax: (+) _____

Signature : _____ Date: _____

(I agree to the Terms and Conditions of Booking)

CONFERENCE FEES

GOVERNMENT, MILITARY AND PUBLIC SECTOR/AGENCY
Individual Full Conference
(includes 3 day conference, conference proceedings, keynote, exhibition, networking reception, coffee breaks and 2 lunches)

- ☐ Paid before 11th February 2026 ..... $195
- ☐ Paid on or after 11th February 2026 ..... $295

OPERATORS/OWNERS OF INFRASTRUCTURE
Individual Full Conference
(includes 3 day conference, conference proceedings, keynote, exhibition, networking reception, coffee breaks and 2 lunches)

- ☐ Paid before 11th February 2026 ..... $195
- ☐ Paid on or after 11th February 2026 ..... $295

COMMERCIAL ORGANISATIONS
Individual Full Conference
(includes 3 day conference, conference proceedings, keynote, exhibition, networking reception, coffee breaks and lunch)

- ☐ Paid before 11th February 2026 ..... $595
- ☐ Paid on or after 11th February 2026 ..... $895

Exhibitor Full Conference
(includes 3 day conference, conference proceedings, keynote, exhibition, networking reception, coffee breaks and lunch)

- ☐ Paid before 11th February 2026 ..... $295
- ☐ Paid on or after 11th February 2026 ..... $450

Student Full Conference
(includes 3 day conference, conference proceedings, keynote, exhibition, networking reception, coffee breaks and lunch) - Student ID required

- ☐ Paid before 11th February 2026 ..... $195
- ☐ Paid on or after 11th February 2026 ..... $195

- ☐ **Conference Proceedings only** $495
- ☐ **EXHIBITION ONLY** (on-site registration $50) $10

(includes access to exhibition floor only)

Terms and Conditions of Booking

Payment: Payments must be made with the order. Entry to the conference will not be permitted unless payment has been made in full prior to 10th March 2026.
Substitutions/Name Changes: You can amend/change a delegate prior to the even start by notifying us in writing. Two or more delegates may not 'share' a place at an event. Please ensure separate bookings for each delegate. Torch Marketing Co. Ltd. reserve the right to refuse entry.
Cancellation: If you wish to cancel your attendance to the event and you are unable to send a substitute, then we will refund/credit 50% of the due fee less a $100 administration charge, providing that cancellation is made in writing and received before 11th February 2026. Regretfully cancellation after this time cannot be accepted. If we have to cancel the event for any reason, then we will make a full refund immediately, but disclaim any further liability.
Alterations: It may become necessary for us to make alterations to the content, speakers or timing of the event compared to the advertised programme.
Data Protection: Torch Marketing Co. Ltd. gathers personal data in accordance with the UK Data Protection Act 1998 and we may use this to contact you by telephone, fax, post or email to tell you about other products and services.
Please tick if you do not wish to be contacted in future by:

☐ Email ☐ Post ☐ Phone ☐ Fax

PAYMENT DETAILS

(METHOD OF PAYMENT - 10.5% SALES TAX WILL BE ADDED TO FEES.)

☐ Wire Transfer (Wire information will be provided on invoice)

☐ Credit Card
Invoice will be supplied for your records on receipt of the order/payment.

Please fill in your credit card details below:
☐ Visa ☐ MasterCard

All credit card payments will be subject to standard credit card charges.

Card No: _____

Valid From ____ / ____ Expiry Date ____ / ____

CVV Number _____ (3 digit security on reverse of card)

Cardholder's Name: _____

Signature: _____ Date: _____

I agree to the Terms and Conditions of Booking.

Complete this form and email to ciprna@torchmarketing.co.uk

From Situational Awareness to Operational Advantage: The Evolving Role of Live Video in Critical Infrastructure Protection

By Carleton M. "Mickey" Miller, CEO, Vislink Technologies

Introduction: Live Video in a Resilience-Focused Intelligence Environment

Critical infrastructure protection, once defined solely by physical security measures, now requires infrastructure owners and public authorities to operate in an environment characterised by asymmetric risk and the potential for a major failure cascade, all the while operating under heightened public scrutiny. Climate-related disruption, supply chain fragility, and hybrid security threats have increased the pressure on operators to detect, assess, and respond to incidents with greater speed and confidence.

Situational awareness in this context is increasingly intelligence-led, often on a multi-agency level, and built through a fusion of sensor data, supervisory control systems, geospatial data, and human reporting. Live video has emerged as a critical enabler within this ecosystem, providing real-time visual confirmation that supports and contextualises other sources of information, enabling

World Border Security Congress

14th-16th April 2026

Vienna, Austria

www.world-border-congress.com

Developing Border Strategies Through Co-operation and Technology

SAVE THE DATES

Austria's border security faces a complex set of challenges, largely stemming from its geographical location and its participation in the Schengen Area. A primary concern is managing irregular migration flows, which fluctuate significantly due to geopolitical instability in various regions. This puts pressure on Austria's capacity to effectively screen and process asylum seekers.

The inherent nature of the Schengen Area, while facilitating free movement, also presents vulnerabilities. The potential for secondary migration, where individuals move from one Schengen state to another, necessitates close cooperation with neighbouring countries. However, differing national policies and capacities can complicate these efforts.

Furthermore, the rise of transnational crime, including human trafficking and smuggling, adds another layer of complexity to border security. Austrian authorities must balance the need for stringent controls with the imperative to uphold human rights and international obligations.

The evolving security landscape, with threats such as terrorism and hybrid warfare, also requires constant adaptation of border security measures. This necessitates investment in advanced surveillance technologies and enhanced intelligence sharing. The need to maintain public confidence in border security, while respecting the principles of open borders within the EU, creates a delicate balancing act for Austrian policymakers.

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.

Join us in Vienna, Austria on 14th-16th April 2026 for the next gathering of international border security, protection and migration management professionals.

www.world-border-congress.com

for the international border management and security industry

Co-hosted by:

To discuss exhibiting and sponsorship opportunities and your involvement contact:

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

Bruce Bassin
Americas
E: bruceb@torchmarketing.co.uk
T: +1 702.600.4651

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

Supported by:

Media Partners:

Emergency Response helicopter treating a forest fire – airborne video can support operations in dangerous environments by providing commanders with a visual overview of major incidents.

faster decision-making.

Rather than functioning as a standalone surveillance capability, live video strengthens resilience by improving understanding during periods of uncertainty of emergency response. It allows decision-makers to visualise evolving conditions, validate intelligence, and agree on operational actions as needs evolve.

A Shift from Retrospective Evidence to Real-Time Risk Assessment

For many years, video in critical infrastructure environments has been used in retrospective analysis. Live video has been hard to implement, hampered by connectivity, technology, or security issues.

However, advances in transmission resilience and network integration have now repositioned live video as a vital operational risk-management tool. In an emergency, visual information enables operators or AI-enabled decision support systems to rapidly assess scale, severity, and potential escalation pathways. This reduces reliance on fragmented reports and supports earlier, more proportionate intervention, while also reducing risk to personnel who might need to make live assessments.

For critical infrastructure operators, live video reduces ambiguity, providing clarity where needed, enabling faster intelligence sharing and decision-making to protect assets, maintain service continuity, and safeguard public safety. The previous burden of requiring live human observation is increasingly being relieved by AI, which enables deeper real-time analysis across datasets, making it even more critical.

This shift is further reinforced by improvements in video quality and resolution. The increasing availability of higher-resolution formats, including 4K, provides a richer visual dataset than legacy surveillance systems were ever able to deliver. For both human operators and agentic AI systems, clearer imagery enables more accurate detection, classification and assessment of activity, conditions and anomalies. In a critical infrastructure context, this additional visual fidelity supports more reliable interpretation of events, reduces false positives, and allows automated systems to extract greater operational insight from live video feeds.

Live Video Perspectives Across Distributed Infrastructure

By their nature, critical infrastructure systems are widely distributed - even across international borders - and often in remote locations. The effectiveness of live video is heightened by the ability to draw insight from different vantage points and asset types.

Elevated and Aerial Perspectives:

Elevated viewpoints from manned aircraft or unmanned systems provide wide-area visibility across critical infrastructure such as pipelines, rail networks, coastlines, and flood defences. These perspectives are particularly valuable during natural disasters or environmental incidents, where ground access may be restricted, and conditions can change rapidly. At these times, aerial video supports impact assessment, prioritisation of response activities, and coordination between infrastructure operators and civil authorities.

Mobile and Deployable Video Assets:

Mobile video deployed via

inspection teams or emergency crews provides close-range situational awareness during incidents that evolve dynamically. These feeds support tactical decision-making while enabling commanders to maintain strategic oversight from control rooms or emergency coordination centres.

Fixed Infrastructure Monitoring:

Fixed cameras at substations, transport hubs, ports, and other critical nodes provide continuity and baseline awareness. When integrated into live operational workflows, these feeds enable operators to detect deviations from normal conditions and track incident progression in real time.

Supporting Decision-Making and Continuity of Operations

A central objective of critical infrastructure protection is maintaining continuity of essential services when under actual or suspected threat. Live video contributes directly to this objective by supporting fast, informed decision-making at both operational and strategic levels.

Visual confirmation enables infrastructure operators and authorities to assess whether incidents are real, contained, or at risk of escalation, informing decisions on secondary operations such as controlled shutdown and public communications. In critical infrastructure environments, these decisions can also be pivotal in preventing localized incidents from cascading into wider system failures across interconnected assets.

From a tactical perspective, visual

Control Room Image: High quality 4K video can be streamed in realtime to the operations control room of any CNI location, enabling rapid environmental analysis and to inform future decision making

information reduces cognitive load during high-pressure situations. By presenting clear evidence of conditions and agentic situational assessment, as they are, it reduces the need for interpretation or clarification, supporting clearer judgment and reducing the likelihood of delayed or overly conservative responses that can exacerbate disruption.

Integration with Command, Control, and Information Systems

Modern CIP operations rely on integrated command, control, and coordination environments. Live video increasingly functions as a data layer within these systems, supplementing and engaging with existing information sources.

When aligned with geospatial platforms, asset management systems, and incident logs, video provides context to the common operating picture. This integration supports cross-organisational coordination, particularly where infrastructure incidents require emergency response involving multiple operators, public safety services, and regulatory bodies.

Underpinning this integration is the growing reliance on proven, mission-critical communications platforms, such as RF and operator-controlled cellular networks, which are increasingly being designed for assured performance and resilience in critical infrastructure environments.

Resilience, Communications Assurance, and Security Considerations

Incidents affecting critical infrastructure frequently occur under degraded communications conditions. Severe weather, network congestion, or physical damage can all disrupt connectivity at precisely the moment when situational awareness is most critical.

The ability to sustain live video under these conditions is a core element of both everyday operational robustness and disaster response. For infrastructure operators and public authorities, resilience depends not only on having access to live video

Military user in the field: Where necessary, live video streams can be securely streamed with partner agencies or law enforcement teams, to ensure that any dangerous situations are handled with the best intelligence to hand.

but also on the ability to sustain it reliably under adverse conditions.

That said, live video also represents sensitive operational information. Protecting its integrity is essential to maintaining trust between stakeholders.

To this end, advances in technology, including diversified connectivity paths, have helped to ensure that visual intelligence remains available during peak demand or partial outages. Software-defined network techniques help maintain that intelligence edge.

Modern systems also ensure high levels of encryption and robust access controls to ensure that live video is a key element in strengthening resilience and enabling response, rather than introducing new vulnerabilities.

Rather than relying on a single network or bearer, modern approaches increasingly combine proven mission-critical communications technologies to provide layered assurance against failure. Traditional RF-based links continue to play a vital role in critical infrastructure environments due to their predictability, controlled spectrum usage, and independence from public networks. These characteristics make RF particularly valuable during large-scale incidents where public infrastructure may be impaired or unavailable.

At the same time, the introduction of mission-critical capability private and public cellular technologies has introduced new options for resilient connectivity. Private and operator-controlled 5G deployments offer dedicated capacity, quality-of-service controls, and network isolation, enabling infrastructure operators and emergency authorities to maintain video connectivity even during periods of extreme demand.

When combined with other bearers, such as licensed RF or satellite backhaul, these platforms provide redundancy and continuity rather than single points of failure.

This multi-layered approach supports manageable degradation rather than abrupt loss of capability. If one connectivity path becomes constrained or unavailable, video services can be maintained through alternative routes, preserving situational awareness and operational continuity.

From a resilience planning perspective, this represents a significant shift away from brittle communications architectures toward adaptive, fault-tolerant systems designed to operate through disruption.

Security considerations remain central to this evolution. Live video used in critical infrastructure operations often contains sensitive information about asset vulnerabilities, response tactics, or public safety activities.

Taken together, these developments mean that live video is no longer constrained by the limitations that once restricted its use in mission-critical environments. By leveraging trusted platforms, agentic AI, diversified connectivity, and robust security practices, infrastructure operators can now treat visual intelligence as a resilient, dependable component of their communications assurance strategy.

Conclusion: Visual Intelligence as a Resilience Enabler

Live video has become a vital

capability within modern critical infrastructure protection. Providing real-time visual context enhances situational awareness, supports confident decision-making, and improves coordination in complex operational environments.

As infrastructure systems face increasing stress from environmental, technical, and security-related threats, resilience will depend on the ability to understand incidents as they unfold. Integrated, secure live video, used in conjunction with other intelligence and visualisation tools, plays a central role in enabling this understanding and supporting the continuity of essential services.

Carleton M. "Mickey" Miller was named CEO of Vislink Technologies in January 2020. He has over 25 years' experience creating and building growth businesses in the technology and communications industries. He has a proven track record in delivering results, from start-ups to Fortune 100 companies, in both growth and turnaround situations. Mickey brings the combination of strategic and organizational ability to lead billion-dollar organizations and the entrepreneurial drive and creativity for mid and small-cap companies.

When Leadership Becomes the Vulnerability: Executive Decision Failure in Critical Infrastructure

When critical infrastructure fails, organizations instinctively search for technical explanations and operational errors. Systems underperformed. Procedures were unclear. Personnel made mistakes. These narratives are familiar and reassuring, because they suggest failure was accidental or unforeseeable. In many cases, it was neither. The most significant vulnerabilities in critical infrastructure today

Jason D. Wallis, Chief of Police for a major U.S. port authority

are not technical or tactical, they are the predictable outcome of executive decision-making.

Across sectors, senior leaders speak fluently about resilience while consistently making decisions that undermine it. Plans are written. Assessments are commissioned. Frameworks are adopted. Yet when systems are stressed, organizations reveal brittle governance, fragmented

authority, and an inability to act decisively. This is not a failure of planning or awareness. It is a failure of leadership, rooted in choices made well before an incident ever occurs.

One of the most damaging patterns is the deliberate diffusion of accountability. Executives construct governance models that emphasize coordination over command and consensus over ownership. Committees proliferate. Decision authority is shared, conditional, or undefined. Risk becomes a collective abstraction rather than an individual responsibility. This approach is often defended as inclusive or collaborative governance. In practice, it functions as institutional risk avoidance. When decisive action is required, no one is clearly empowered to act, and no one is clearly accountable when action is delayed.

Critical infrastructure incidents do not fail because too few people were consulted. They failed because decisions were not made. Yet many executives remain reluctant to grant or defend real authority at the operational level, particularly when decisions carry legal, political, or reputational exposure. Leaders expect decisiveness from below while preserving deniability above. When outcomes are uncertain, authority is constrained. When outcomes are negative, responsibility is displaced. This dynamic is not accidental. It is structural.

Equally corrosive is the normalization of deferred risk. Maintenance is postponed. Training is reduced. Staffing is optimized. Security investments are delayed. Each decision is framed as reasonable, temporary, or fiscally responsible. Viewed in isolation, these choices appear manageable. Taken together, they hollow out resilience. The absence of immediate failure is mistaken for success, reinforcing behaviors that ensure future breakdowns. Risk does not disappear, it accumulates.

This leadership failure is especially evident in how organizations address insider risk. Despite repeated, well-documented incidents across critical infrastructure sectors, executive engagement remains shallow. Insider threat is treated as a peripheral issue, delegated to compliance programs or employee assistance resources, rather than confronted as a core security and governance challenge. Leaders avoid the uncomfortable reality that access, stress, grievance, and mental health intersect directly with operational risk. This avoidance is not benign. It leaves organizations exposed to one of the most predictable and preventable failure modes.

These outcomes are not driven by ignorance or incompetence. They are the product of governance systems designed to minimize executive exposure rather than operational risk. Leaders are rewarded for managing perception, aligning stakeholders, and avoiding controversy. Critical infrastructure, however, does not fail on perception. It fails on decisions that were delayed, diluted, or never made.

Resilience is not created by documentation, frameworks, or post-incident lessons learned. It is created by leaders who accept ownership of risk, delegate authority clearly, and stand behind difficult decisions before they are tested. Anything less is performative resilience reassuring on paper and ineffective under pressure.

The uncomfortable truth is this: executive decisions actively shape the threat environment. Every deferred investment, every ambiguous authority structure, every avoided conversation about human risk creates exploitable conditions. These outcomes are not unpredictable. They recur because leadership behavior does not change.

Critical infrastructure resilience is not failing because frontline personnel lack capability or commitment. It is failing because leadership too often prioritizes comfort, consensus, and deniability over consequence. Until executives acknowledge that their own decisions are among the most significant sources of risk, critical infrastructure protection will remain reactive, explaining failure after the fact rather than preventing it.

Jason D. Wallis is Chief of Police for a major U.S. port authority, with nearly three decades of experience in aviation security, critical infrastructure protection, and high-risk incident leadership.

Link11 Identifies Five Cybersecurity Trends Set to Shape European Defense Strategies in 2026

Link11, a European provider of web infrastructure security solutions, has released new insights outlining five key cybersecurity developments expected to influence how organizations across Europe prepare for and respond to threats in 2026. The findings are based on analysis of current threat activity, industry research, and insights from the Link11 European Cyber Report, alongside broader market indicators such as PwC's Global Digital Trust Insights 2026.

Cybersecurity is entering uncharted territory as the global threat landscape evolves at high speed. Geopolitical instability, fractured supply chains, and rapid advances in artificial intelligence are reshaping how cyber operations are conducted. According to PwC's Global Digital Trust Insights 2026, geopolitical uncertainty has become one of the strongest drivers of increased cybersecurity investment, while many organizations continue to underinvest in proactive measures such as monitoring, testing, and hardening. These conditions leave critical gaps that increasingly sophisticated attackers are able to exploit.

Five Key Cybersecurity Trends for 2026:

1. DDoS Attacks Will Increasingly Be Used as Diversion Tactics

Link11 expects a marked rise in DDoS attacks in 2026. These attacks will not primarily be launched to disrupt services, but rather to draw attention away from more damaging activities occurring simultaneously. While IT teams are focused on keeping systems online, attackers may exploit the distraction to infiltrate networks, steal sensitive data, or deploy covert malware. These hybrid operations often remain undetected until long after the initial DDoS wave has been mitigated. For European organizations, this underscores the need for incident response frameworks that treat any DDoS alert as a potential precursor to a broader, multi-vector intrusion.

2. API-First Architectures Increase Exposure to Misconfigurations and Business Logic Abuse

APIs will continue to be the backbone of Europe's digital services, including financial platforms, e-commerce, and public-sector portals. As they grow in number and complexity, improperly secured or undocumented APIs are becoming one of the most attractive entry points for threat actors. These attackers exploit weaknesses through automated scraping, credential-stuffing campaigns, or by targeting high-value endpoints designed for critical business operations. In 2026, organizations that rely on large ecosystems of internal and external APIs will face rising risks of data leakage, process manipulation, and unauthorized access.

3. Integrated WAAP Platforms Overtake Fragmented Web Security Architectures

Traditional, siloed web security tools – such as separate web application firewalls (WAFs), standalone distributed denial-of-service (DDoS) filters, and isolated bot management systems – are no longer adequate against multi-layer attacks. The shift toward consolidated web application and API protection (WAAP) platforms will accelerate across Europe in 2026. By correlating signals across protection layers, integrated WAAP systems can detect subtle anomalies and block sophisticated attacks that single-layer solutions would miss. This architectural convergence is essential for organizations operating in hybrid cloud environments or managing large-scale digital platforms.

4. AI-Driven DDoS Mitigation Becomes Essential Against Hyper-Scale Attacks

DDoS attacks have evolved dramatically in terms of both scale and complexity. Massive IoT botnets and automated infrastructures can generate near-instantaneous traffic spikes, so rule-based mitigation is insufficient. By 2026, effective protection will depend on AI and behavioral analysis to distinguish legitimate traffic from dynamic attack patterns, enabling autonomous mitigation in milliseconds. To maintain service availability and reduce operational disruptions, European organizations will increasingly adopt AI-first DDoS defenses.

5. Regulatory Pressure Intensifies as Cybersecurity Oversight Expands Across Europe

Regulatory frameworks such as NIS2 and DORA, as well as emerging national requirements, will impose strict expectations on businesses operating in the European market. Organizations must prepare for rapid breach reporting obligations, often within 24 to 72 hours, and significantly heightened scrutiny of supply chain security. Additionally, governments are moving toward stronger accountability for software vendors through Secure-by-Design mandates and mandatory Software Bills of Materials (SBOMs). For many organizations, compliance will evolve from an annual task to an integral operational practice.

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

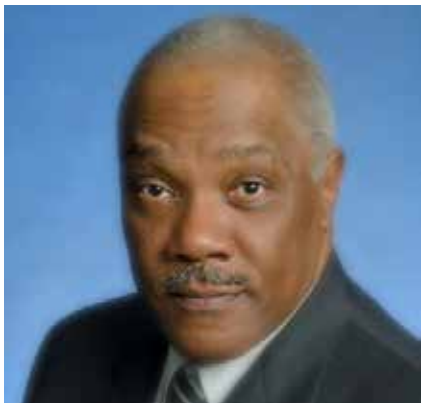
For further details and to join, visit **www.cip-association.org** and help shape the future of this increasingly critical sector of national security.

We look forward to welcoming you.

John Donlon **QPM, FSI**
Chairman
IACIPP

The Critical Infrastructure Facility Owner's oversight of the protection officer and the Cybersecurity workforce competencies

This article examines the crucial role of critical infrastructure facility owners in supervising protection officers and cybersecurity personnel, using competency models from the Competency Model Clearinghouse. Owners must ensure both groups have the required skills to handle physical and cyber threats, supporting a unified security approach and ongoing professional growth. This comprehensive oversight is essential to safeguard



Dr. Ron Martin, Professor of Practice, Capitol Technology University

infrastructure and maintain public trust.

Over the years, I have managed security for critical infrastructure and faced challenges in recruiting skilled personnel. Countries and their jurisdictions set educational and competency requirements for these roles to ensure facility protection. As an owner/operator, overseeing both physical and cyber security is essential, with staff needing relevant skills

and abilities for critical tasks. The U.S. Department of Labor's Competency Model Clearinghouse aims to clarify the competencies needed for a globally competitive workforce.

What is a competency?

A competency is the capability to apply or use a set of related knowledge, skills, and abilities required to successfully perform "critical work functions" or tasks in a defined work setting.

What is a competency model?

A competency model is a collection of multiple competencies that together define successful performance in a defined work setting. A model provides a clear description of what a person needs to know and be able to do – the knowledge, skills, and abilities – to perform well in a specific job, occupation, or industry.

Each has three competency components:

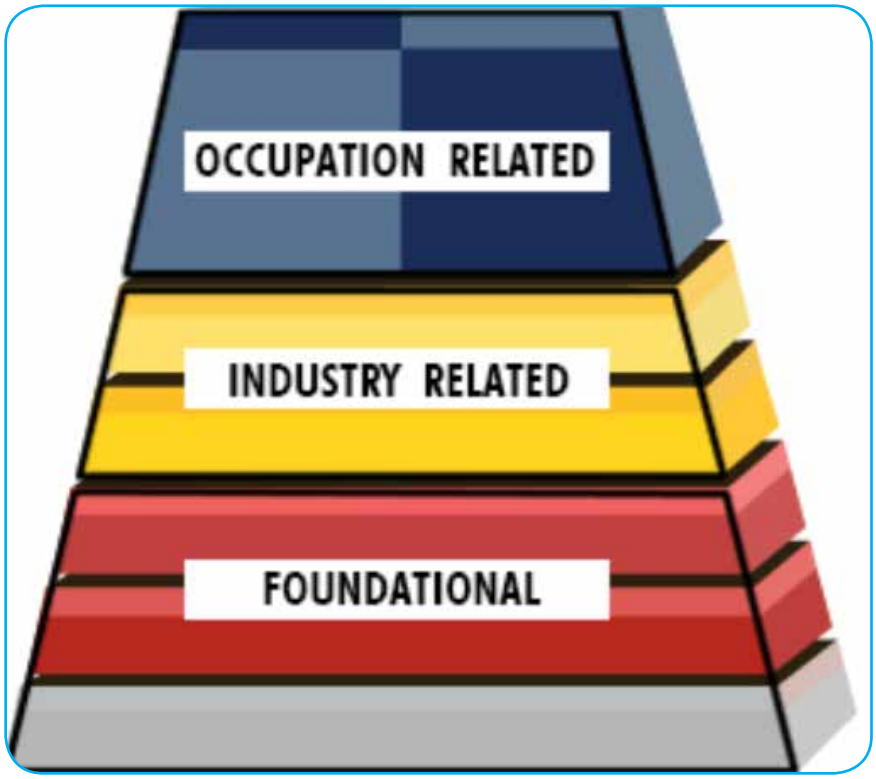
Foundational: These competencies provide the foundation for success in school and in the world of work.

Industry Related: Describe cross-cutting, industry- and sector-wide skills, knowledge, and abilities

Occupational: Identify and specify occupational competencies to define workplace performance, design competency-based curricula, or set requirements for credentials

About the Competency Models | Get Started | Competency Model Clearinghouse

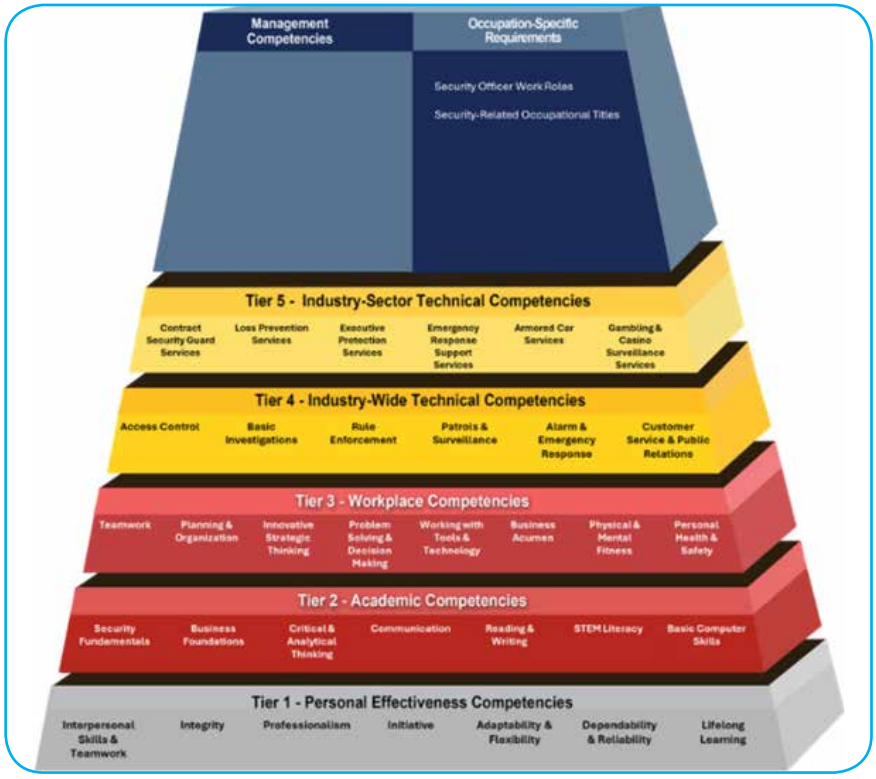
Two competency models that are important to the critical infrastructure owner/operator are

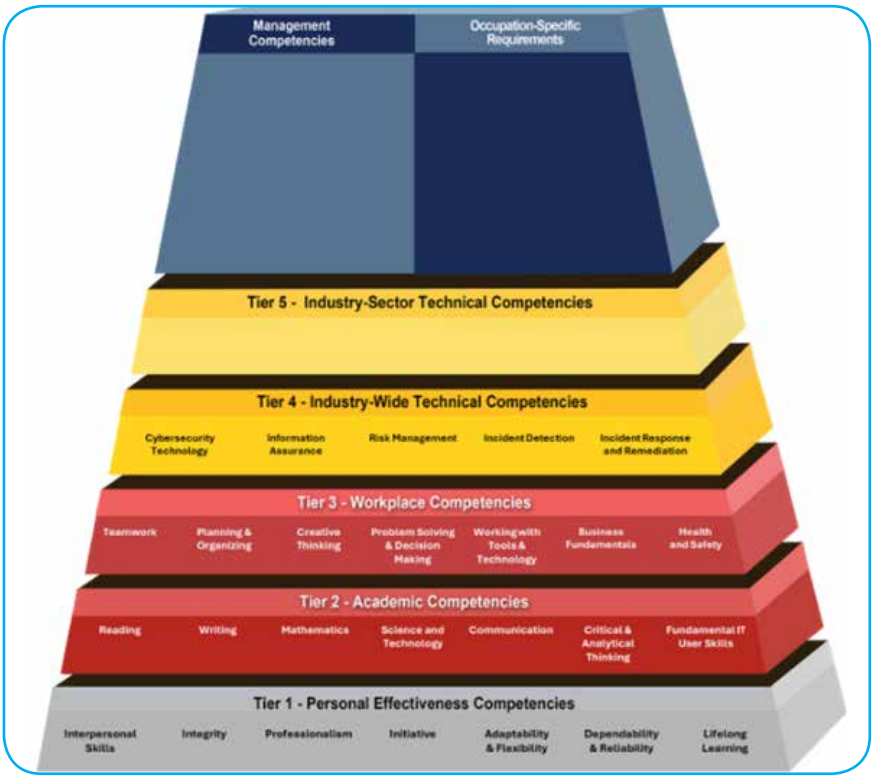


the Security Officers and Patrol Services, and the Cybersecurity Competency Models.

Security Officers and Patrol Services | Industry Models | Competency Model Clearinghouse

The International Foundation for Protection Officers developed the Security Officers and Patrol Services Competency Model. Collaborating with security subject matter experts from around the world since 1988, they have published numerous





publications on protection officer competencies.

The competency model framework for Security Officers and Patrol Services was developed through a collaborative effort involving the Employment and Training Administration (ETA) and leading industry organizations. It identifies the soft skills and foundational competencies, as well as the technical knowledge, skill, and abilities, needed by professionals entering the Security Officers and Patrol Services field.

The Security Officers and Patrol Services Competency Model framework defines the latest skills and knowledge requirements needed by individuals who provide security officer duties to protect their organization's assets, regardless of the industry sector within which they work. The model framework incorporates competencies identified through global research completed in 2021 and is supported by the numerous editions of IFPO's "The Professional Protection Officer," which is the text for IFPO's Certified Protection Officer (CPO) designation, written and updated by security subject matter experts from around the world since 1988. IFPO will work with industry experts and partners to ensure that the model framework will continue to be updated to reflect the evolving competency requirements of the industry.

In 2025, the foundational tiers of the model were updated to align with changes in the Building Blocks Model.

Cybersecurity | Industry Models | Competency Model Clearinghouse

The second model is the Cybersecurity Competency Model. The U.S. National Institute of Standards and Technology (NIST) Leads the National Initiative for Cybersecurity Education (NICE).

The Cybersecurity Competency Model below provides a simplified overview of the detailed competencies identified in the Workforce Framework for Cybersecurity (NICE Framework) and is intended to direct users to the many available resources associated with that framework.

The NICE Framework is a reference resource for identifying, recruiting, developing and maintaining cybersecurity talent. The framework provides a common language to categorize and describe cybersecurity work that will help organizations build a strong labor force to protect systems and data. The NICE Framework was developed by NICE, led by NIST in the U.S. Department of Commerce, with support from the U.S. Departments of Defense and Homeland Security, and is the culmination of many years of collaboration between industry, government, and academia.

NICE | workforce framework for cybersecurity

Given the nature of and pace of change in cybersecurity, please visit the NICE Framework to keep up-to-date on the latest competencies.

For those who prefer to use the Competency Model Clearinghouse downloadable worksheets to conduct employer needs analysis, perform gap analysis, develop curriculum, or align credentials, use the link below for Tiers 1-4, which were developed with input from NICE. As the NICE Framework is updated on an ongoing basis, in 2024, changes to remove Tier 5 from the Competency Model Clearinghouse model were made.

For detailed content on Tier 5 and above, Industry-Sector Functional Areas, visit the NICE Framework for the most current competencies and other resources. In 2025, the foundational tiers of the model were updated to align with changes in the Building Blocks Model.

This article summarizes the three core components of competency models—foundational, industry-related, and occupational competencies—which are essential for success in education and the workforce. Foundational competencies cover basic skills; industry-related competencies address broad-sector abilities; and occupational competencies define role-specific standards. Two key models for critical infrastructure are the Security Officers and Patrol Services Competency Model and the Cybersecurity Competency Model. The Security Officers model outlines vital skills for protection officers, while the Cybersecurity model, based on NIST's NICE Framework, supports the development of a skilled cybersecurity workforce. These models help shape competency-based curricula, set credential standards, and improve talent development across critical infrastructure sectors.

Disaster losses are far higher than insurance industry estimates as invisible impacts go uncounted

The true cost of disasters is significantly underestimated worldwide, as losses to health, livelihoods, ecosystems, and long-term development remain largely unmeasured.

Wildfires burned through 390 million hectares in 2025 – equivalent to 92% of the European Union's land area – yet the costliest event of the year, the January fires in and around Los Angeles, burned just 23,000 hectares while causing around USD 40 billion in insured damages.

Global disaster losses reached an estimated USD 224 billion in 2025, with less than half insured, Munich Re reported today. The January 2025 Los Angeles wildfires dominated headlines as the costliest single event of the year, but even in data-rich settings, large portions of wildfire damage fall outside official accounting. In many regions where fires burn most extensively, data gaps are far wider.

"Every year, institutions across the insurance industry, international organisations, and think tanks publish aggregate figures on disaster losses," said Kamal Kishore, Special Representative of the UN Secretary-General for Disaster Risk Reduction. "But we need to do much more to improve the quality of data on disaster-related damages and losses."

More than half of wildfire events recorded in international databases lack information on economic losses or the number of people affected. Reliable data is concentrated in a small number of high-income regions, while fire-prone areas across Africa and parts of Asia remain largely invisible in global risk metrics.

"Even when data exists, it is often focused on direct impacts and not enough on indirect impacts," Mr Kishore said. "This is a major gap in how disaster risk is understood."

Wildfire risk likely to continue to rise as settlements and high-value assets expand into fire-prone areas, increasing exposure even where total burned area has declined. Yet in many countries, wildfire risk is still missing from national risk profiles, investment decisions, and fiscal planning.

"We have ample data for large, visible disasters," Kishore said, "but data on small- and medium-scale events remains patchy, particularly for slow-onset and creeping hazards."

Unless the full range of wildfire impacts is measured – including long-term health effects, environmental degradation, and economic disruption – losses will continue to rise and prevention will remain underfunded.

Making these invisible costs visible is essential to reducing future risk and strengthening resilience as climate-related disaster risks continue to rise globally.

The Need for Level 0 (Process Sensor and Actuator) Cybersecurity Training

bY Joe Weiss, PE, CISM, CRISC, Managing Partner, Applied Control Solutions LLC

Critical infrastructures can't be cybersecure or safe if the Purdue Reference Model Level 0 devices can't be trusted. Level 0 devices (process sensors measuring pressure, level, flow, temperature, voltage, current, etc. and associated actuators) form the foundation of physical operations and are indispensable to process safety, reliability, and productivity across critical infrastructures. Level 0 devices are assumed to be uncompromised, authenticated, and correct with associated cyber forensics. However, Level 0 devices have no cybersecurity, authentication, cyber forensics and are 100% trusted. Consequently, Level 0 devices cannot authenticate signals, validate integrity, or provide cyber forensic evidence. This reality creates a profound regulatory and operational challenge because modern cybersecurity frameworks assume these devices possess protections that are technologically infeasible today.

These erroneous Level 0 assumptions are deeply embedded in the design of industry cybersecurity frameworks. The lack of embedded cybersecurity in these devices forces a fundamental reexamination of current regulatory frameworks such as NERC CIP, ISA/IEC 62443-4-2, NIST SP 800-82, API, AWWA, NEI-0809, CISA, TSA, and EPA

as they do not provide adequate compensating controls for Level 0 devices. Additionally, there is no OT cybersecurity training for Level 0 devices. Policymakers must acknowledge that existing regulations presuppose technological capabilities are years away from being realized. Until next generation cybersecure process sensors become available at scale, governments and industries must rely on process sensor monitoring at the physics level, enhanced operational practices, appropriate process sensor cybersecurity training, and updated safety standards to protect critical infrastructures. Failing to address the Level 0 gap perpetuates a dangerous illusion of security and safety while the most vulnerable components of control systems remain exposed. The path forward requires pragmatic regulation aligned with engineering realities and a commitment to accelerating the development of secure, resilient process sensor and actuator technologies and appropriate training.

Real-world events, including accidental compromises, equipment failures, and malicious manipulation have demonstrated that process sensors and actuators can and have been compromised, sometimes with catastrophic consequences. The ultimate irony is that the insecure field devices were themselves manufactured using systems with insecure field devices. Where does the "root of trust" start?

Process sensor cybersecurity issues are not new, and I expected they would have been addressed by now. However, that is not the case.

IEC 62443-4-2 provides an important framework for device cybersecurity, but Level 0 devices predate these requirements, and they do not provide the basic capabilities the standard assumes. This was validated by a special ISA subcommittee in 2017 and by a dedicated review by ISA 84.09 (the intersection of cybersecurity and process safety) in 2021. Many sectors are using ISA-62443 or a sector-specific modification. This means that multiple sectors that rely on the 62443 standards are not adequately addressing cybersecurity of Level 0 devices.

In early February 2025, the Cybersecurity and Infrastructure Security Agency (CISA) advertised that they were offering control system cybersecurity training at a college site. Idaho National Laboratory (INL) acknowledged the training did not have specific training on field controllers or field devices. In late February 2025, EPA stated that IT cybersecurity should be applied to Level 0 devices even though IT security policies and recommendations may be inappropriate and could even damage the Level 0 devices.

In November 2025, INL held a two-hour training course on using Cyber Informed Engineering (CIE) on a water plant. Process sensors were mentioned, but even that mention was minimized by statements that erroneous sensor readings could be compensated for by using CIE.

In November 2025, SANS published the results of their survey on Linked-in: SANS State of OT Security 2025: What the Data Tells Us. The SANS report did not distinguish between Level 0 and Level 1 equipment, and they are not the same. This lack of distinction by practitioners is itself evidence that current OT cybersecurity training does not cover Level 0 in a meaningful or differentiated way. This is a clear message that OT cybersecurity experts are not being adequately taught the unique cybersecurity issues with Level 0 devices.

The lack of Level 0 cyber security capabilities requires compensating controls. However, there is no dedicated Level 0 cybersecurity training and existing cybersecurity training for OT networks is not applicable. Additionally, the lack of process sensor cybersecurity training has led to the gap in control system cybersecurity requirements in procurement requirements. This perpetuates the Level 0 vulnerabilities across new projects and retrofits.

Level 0 cybersecurity training needs to include relevant cybersecurity training as well as address the design and operation of appropriate Level 0 devices and their cyber vulnerabilities. The training should include examples of both unintentional and malicious Level 0 cyber incidents. The training needs to be delivered by experts in Level 0 devices and cybersecurity.

In summary, with the lack of Level 0 cybersecurity, authentication, and appropriate training, critical infrastructure OT cybersecurity is built on a foundation of sand.

Why recovery speed shapes resilience?

On 12 January 2010, a magnitude 7.0 earthquake struck Haiti, claiming an estimated 300,000 lives, displacing millions, and devastating much of the country's urban infrastructure. Six years later, an earthquake of comparable magnitude hit Kumamoto, Japan. While the physical shock was severe, the human toll was far lower: around 200 fatalities, fewer displaced families, and significantly less long-term damage.

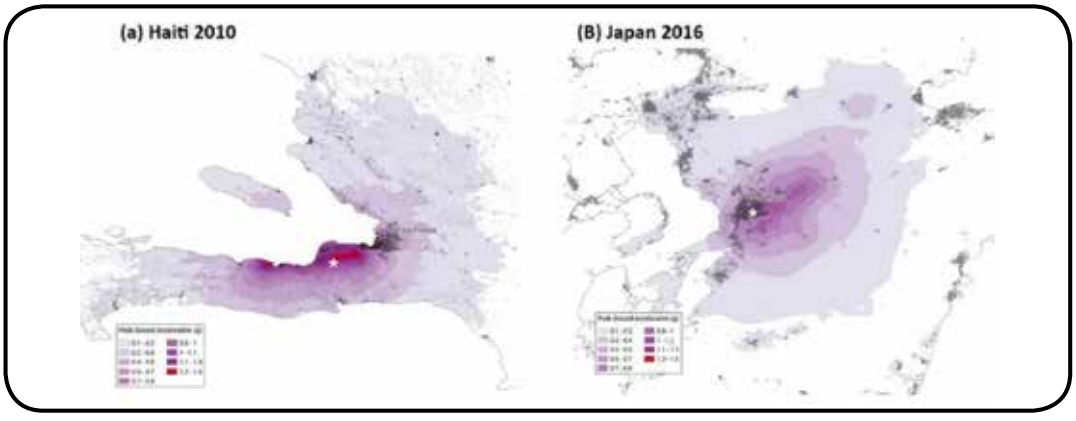
The difference was not only the hazard itself. It was what came after.

In Haiti, five years after the earthquake, an estimated 80,000 people were still displaced, and even today-more than a decade later-parts of the housing stock and critical infrastructure remain unreconstructed. In Japan, electricity and gas were fully restored within 11 days, and airports resumed operations within weeks. Recovery began immediately, and it moved fast.

This anniversary is not only a moment of remembrance. It is a reminder that disasters do not end when the ground stops shaking. For families who lose homes, livelihoods, or savings, the true dividing line is recovery speed-how quickly people can rebuild, restore income, and return to a dignified standard of living. When recovery is slow, losses compound, poverty deepens, and development setbacks can last for generations. When recovery is fast, resilience becomes real.

Recovery speed refers to the rate at which households rebuild destroyed assets or restore their income sources after a disaster, until they regain at least their pre-disaster consumption level.

The same pattern holds at the national level. Studies by the World Bank show that low-income countries take 56% longer to recover their consumption than high-income countries. Low consumption levels not only affect the economy but also family well-being. When households lack access to liquidity, credit, or social protection, they are forced to cut essential spending, which amplifies the human cost of asset losses and slows down recovery.

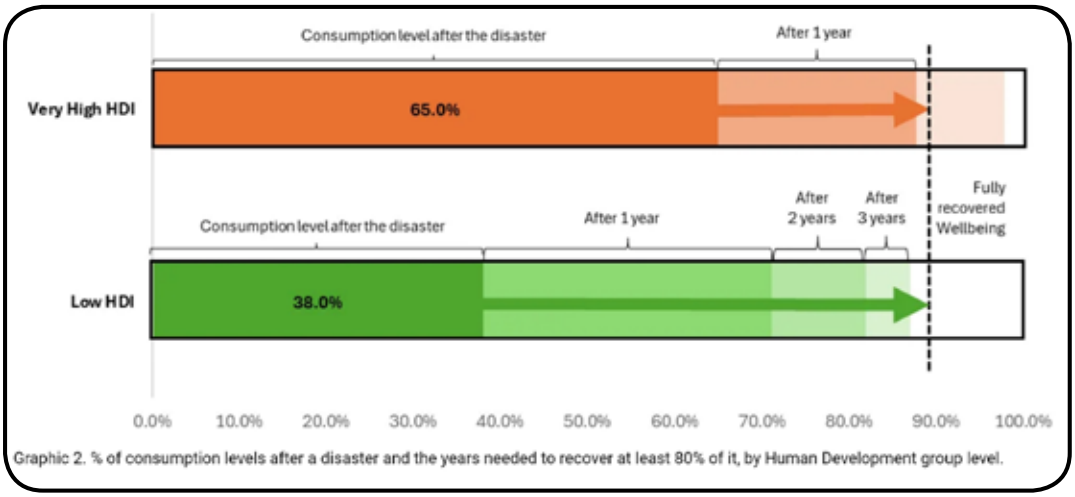


This gap is clearly illustrated by Japan and Haiti. Although both can experience a hazard of similar magnitude, households in Japan typically regain their pre-disaster consumption within about 1.5 years, while in Haiti recovery can take up to four decades. The difference lies in the policies enabling recovery. Japan's rapid recovery reflects decades of investment in comprehensive social protection, strong insurance coverage, and coordinated recovery planning, all of which protects households and accelerate reconstruction.

The chart above shows how recovery time increases as human development (HDI) levels decrease. While high-HDI countries often recover household consumption within a year, low-HDI countries may take three years or more, and in fragile contexts, such as Haiti, far longer.

How can we accelerate recovery?

Policies that integrate disaster and climate risk into fiscal frameworks, such as adaptive social protection, risk-based budgeting, and contingent financing, can dramatically cut recovery time. This means resilience must be a budgetary principle, not just a humanitarian objective. At the same time, recovery speed depends on national recovery readiness: the



Graphic 2. % of consumption levels after a disaster and the years needed to recover at least 80% of it, by Human Development group level.

ability to plan, finance, and coordinate recovery in a timely, inclusive, and effective way.

Embedding risk analytics into national budgets and investment pipelines, pre-identifying vulnerable households, and putting governance, coordination, and financing mechanisms in place before disasters occur can deliver the highest well-being returns per dollar invested.

In June 2025, G20 countries recognized the Recovery Readiness Assessment Framework as an important tool to help for governments prepare for faster recovery. The framework provides a concrete roadmap by defining four coreenablers of recovery speed- governance, finance, capacity and data- and highlights why investing in these before a shock occurs is key to reducing recovery time.

Resilience-oriented financial systems and recovery readiness are central to sustainable development. When financial systems, social protection, and recovery plans are aligned, societies can recover faster, protect development gains, and reduce the long-term human cost of disasters.

ADPC Embarks on a New Initiative for Resilient Disaster Recovery in Asia and the Pacific

The Asian Disaster Preparedness Center (ADPC), in collaboration with the United Nations Office for Disaster Risk Reduction (UNDRR) as a partner, is pleased to announce the commencement of a new regional project with the Asian Development Bank (ADB) titled "Enhancing Asia and the Pacific's Readiness for Resilient Disaster Recovery.

The program will work closely with governments in Bangladesh, the Kyrgyz Republic, Mongolia, and Timor-Leste, helping these participating countries conduct structured assessments of their recovery readiness, prepare recovery readiness roadmaps and financial preparedness plans, improve disaster-responsive public financial management systems, and capture lessons from past disaster recovery experiences through nationally led after-action reviews. It will work with the countries to establish regional

cooperation to encourage learning between them, and to develop a common toolkit for learning from past recovery experiences, while facilitating training and capacity-building activities for government officials. By fostering broad stakeholder engagement, including women's groups, at-risk communities, and the private sector, the project seeks to ensure that recovery planning processes are inclusive and participatory.

This initiative comes at a critical juncture as countries in Asia and the Pacific face growing exposure to natural hazards that disrupt development progress and strain public institutions. The need for systems, processes, and capacities in readiness for swift recovery after disasters has been highlighted due to the increasing frequency and intensity of natural hazards across the region. This is particularly important since delays in recovery, often caused by limitations in governance systems, public financial management, financial resources, and fund flow management, as well as implementation capacities, invariably exacerbate the impact of disasters, especially for the most vulnerable groups.

By the end of 2028, participating countries are expected to be better equipped to plan, finance, and manage disaster recovery in ways that are sustainable, gender-responsive, and nationally owned, contributing to stronger resilience across Asia and the Pacific.

CISA Releases Dynamic New Guide for Stadium and Arena Owners to Fortify Operations, Mitigate Vulnerabilities and Elevate Emergency Preparedness

Ahead of a Historic Year of Sports and Entertainment CISA Continues to Work with Industry Partners to Keep Stadiums and Arenas Safe

The Cybersecurity and Infrastructure Security Agency (CISA) released the Venue Guide for Mitigating Dependency Disruptions, a new resource designed to strengthen the resilience of public gathering venues. This guide provides stadium and arena owners and operators with baseline strategies to mitigate the consequences of potential disruptions to four critical lifeline sectors—including Energy, Water and Wastewater Systems, Communications, and Transportation.

CISA developed this guide in close collaboration with government and industry experts from the four lifeline sectors as a concise, actionable resource for stadium and arena owners. Tailored for major public gathering events- such as FIFA World Cup 2026, America 250, and 2028 Summer Olympics, the guide draws on lessons learned from recent disruptions at high-profile public gathering sports and entertainment facilities across the United States and internationally. It equips critical infrastructure stakeholders with a clear understanding of threats to lifeline sectors and provides effective strategies to safeguard operations, reduce vulnerabilities, and enhance preparedness.

"Today's risk environment is rapidly evolving, posing serious threats and disruptions to U.S. critical infrastructure and public gathering venues," said CISA Acting Director Madhu Gottumukkala. "CISA is committed to working hand-in-hand with our government and industry partners to deliver actionable guidance that helps mitigate these risks. This guide empowers venue owners and operators to proactively assess vulnerabilities tied to dependent lifeline services and integrate those insights into contingency planning—ultimately reducing potential consequences and strengthening operational resilience."

The Venue Guide for Mitigating Dependency Disruptions aligns with Executive Order 14234 Establishing the White House Task Force on the World Cup 2026, Executive Order 14239 Achieving Efficiency through State and Local Preparedness, and Executive Order 14328 Establishing the White House Task Force on the 2028 Summer Olympics. This guide assists critical infrastructure and public venue owners and operations with:

- Understanding the lifeline sector dependencies and interdependencies that their venues may rely on;
- Assessing security risks and associated key components of a facility evaluation; and
- Focusing on continued information-sharing and relationship-building with key partners such as local services providers, first responders, and CISA Security Advisors.

"Robust partnerships are essential to safeguarding critical infrastructure and public gatherings. By sharing threat intelligence, risk mitigation strategies, and other vital information, we strengthen our collective ability to anticipate and respond to potential disruptions. CISA's newly released guide empowers venue owners and operators to assess dependencies and implement targeted mitigation strategies," said CISA Executive Assistant Director for Infrastructure Security Steve Casapulla. "We deeply value the insights and collaboration from our government and industry partners across four lifeline sectors, which were instrumental in shaping this timely and practical resource. CISA urges all organizations that host events to review the guide and take proactive steps to enhance infrastructure security and resilience."

Draft NIST Guidelines Rethink Cybersecurity for the AI Era

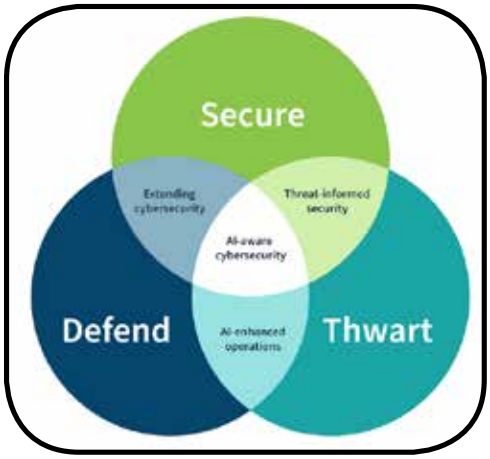
Artificial intelligence (AI) is impacting many organizations' activities, and cybersecurity is no exception. For anyone interested in the opportunities and risks at the intersection of cybersecurity and AI, the National Institute of Standards and Technology (NIST) has released a preliminary draft of its Cyber AI Profile.

The publication, whose full title is the Cybersecurity Framework Profile for Artificial Intelligence (NISTIR 8596), offers guidelines for using the NIST Cybersecurity Framework (CSF 2.0) to accelerate the secure adoption of AI. The profile helps organizations think about how to strategically adopt AI while addressing emerging cybersecurity risks that stem from AI's rapid advance.

The draft resulted from a yearlong effort on the part of NIST cybersecurity and AI experts. Over that time, more than 6,500 individuals have joined the community of interest to contribute to NIST's development of the profile. After releasing an initial concept paper in February 2025, conducting a workshop the following April, and hosting a series of community of interest meetings in the summer, NIST is now releasing the preliminary draft of the profile for a 45-day public comment period.

The Cyber AI Profile centers on three focus areas:

- Securing AI systems: identifying cybersecurity challenges when integrating AI into organizational ecosystems and infrastructure
- Conducting AI-enabled cyber defense: identifying opportunities to use AI to enhance cybersecurity, and understanding challenges when leveraging AI to support defensive operations
- Thwarting AI-enabled cyberattacks: building resilience to protect against new AI-enabled threat



The Cyber AI Profile can help organizations use the CSF to crystallize their cybersecurity goals with respect to AI and CSF 2.0. The profile offers insights to help organizations understand, examine and address the cybersecurity concerns related to AI and thoughtfully integrate AI into their cybersecurity strategies.

NIST Launches Centers for AI in Manufacturing and Critical Infrastructure

The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) has expanded its collaboration with the nonprofit MITRE Corporation as part of its efforts to ensure U.S. leadership in artificial intelligence (AI). Through this award, NIST is investing $20 million to establish two centers to advance the delivery of AI-based technology solutions to strengthen U.S. manufacturing and cybersecurity for critical infrastructure.

The award is an important step in implementing NIST's Strategy for American Technology Leadership in the 21st Century to accelerate the progress of critical and emerging technologies from development to adoption, in close partnership with U.S. industry.

"Our goal is to remove barriers to American AI innovation and accelerate the application of our AI technologies around the world," said Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director Craig Burkhardt. "This new agreement with MITRE will focus on enhancing the ability of U.S. companies to make high-value products more efficiently, meet market demands domestically and internationally, and catalyze discovery and commercialization of new technologies and devices."

The AI Economic Security Center for U.S. Manufacturing Productivity and the AI Economic Security Center to Secure U.S. Critical Infrastructure from Cyberthreats will drive the development and adoption of AI-driven tools, or "agents," in these two national priority areas. The centers will develop the technology evaluations and advancements that are necessary to effectively protect U.S. dominance in AI innovation, address threats from adversaries' use of AI, and reduce risks from reliance on insecure AI.

IAEA and Central Asian Countries Extend Cooperation on Safe Management of Former Uranium Mining Sites

The IAEA has published a new strategic master plan to continue its cooperation with Kyrgyzstan, Tajikistan and Uzbekistan and international organizations on the remediation of uranium legacy sites until 2030.

These uranium legacy sites are former uranium mining, milling and processing facilities from the mid-1940s to the 1990s that were abandoned without plans for safe closure and decommissioning. The IAEA Coordination Group for Uranium Legacy Sites (CGULS) supports countries to safely manage these sites and the residues of radioactive and toxic contaminants to protect people and the environment.

"The new plan, an extension of our collaboration since 2017, focuses on enhancing the regulatory, technical, financial and human resources for the long term management of the remediated sites, according to IAEA safety standards," said Hildegarde Vandenhove, Director of the IAEA Division of Radiation, Transport and Waste Safety.

The plan will guide the future activities of the IAEA, international organizations and collaborating countries, focusing on monitoring, maintenance, record keeping and continuous stakeholder engagement towards the safe and beneficial use of the remediated land.

Under the original plan adopted in 2017, seven uranium legacy sites in Central Asia were designated as high priority for remediation, owing to the risk they posed to nearby communities and the environment. Since then, four out of the seven high priority sites have been remediated — two in Kyrgyzstan and two in Uzbekistan — allowing local communities to use the land safely.

Work continues at a fifth site in Kyrgyzstan, one of the largest and most complex, with remediation expected to continue until 2032. In Tajikistan, one site has been partially remediated and another remains to initiate remediation.

As well as ensuring the high priority sites are managed and reused safely, the new plan encompasses lower priority sites for remediation – sites that present lower risks in terms of environmental, social and economic considerations, and were not remediated under the previous plan.

NSA Releases First in Series of Zero Trust Implementation Guidelines

The National Security Agency (NSA) is releasing the first two products in a series of Zero Trust Implementation Guidelines (ZIGs) to provide practical, actionable recommendations to facilitate the implementation of Zero Trust (ZT).

This series of reports outlines the steps to implement the technologies and processes that support achieving the Target-level ZT Capabilities, Activities, and Expected Outcomes described in the Department of War (DoW) CIO ZT Framework.

The Primer and Discovery Phase are the gateway to ZT implementation, providing guidance and direction to ensure organizations are fully equipped to digest and implement the Phase 1 and Phase 2 ZIGs upon their release.

The Primer outlines the strategy and principles used to develop the ZIGs and provides a holistic approach to maximizing the usage of the series. Notably, the ZIGs are designed to be modular, allowing organizations at different levels of ZT maturity to select and implement the capabilities most relevant to the needs of their environment.

The Discovery Phase is intended to help organizations establish foundational visibility and understand the critical data, applications, assets, and services, as well as access and authorization activity existing within the architecture. The goal of this initial phase is to enable informed prioritization and planning by creating a reliable baseline that supports effective ZT implementation.

System owners, cybersecurity professionals, and stakeholders should review these foundational guidelines to gain a deeper understanding of ZT activities and their organization's operational landscape in preparation for the release of the Phase 1 and Phase 2 ZIGs.

New report explores use of robotics and unmanned systems in the fight against crime

Europol has published The Unmanned Future(s): The Impact of Robotics and Unmanned Systems on Law Enforcement. The report, produced by the Europol Innovation Lab, provides an in-depth analysis of how unmanned systems could change society, crime and law enforcement, and discusses the challenges and opportunities they present.

The report underscores the rapid advancement and integration of unmanned systems in various sectors, including law enforcement. As these technologies become more sophisticated and widespread, they offer new opportunities for law enforcement operations and operational support. However, they also introduce new security threats – such as misuse by criminal and terrorist groups – and regulatory challenges that law enforcement agencies must address to ensure public safety and maintain trust.

One chapter of the report highlights the role of war as a driver for innovation in unmanned systems. Recent conflicts, such as the ongoing Russian war of aggression against Ukraine, have accelerated the development and deployment of advanced unmanned systems. The

lessons learnt from these conflicts are invaluable for law enforcement agencies in Europe as they prepare for the future operating environment.

Some of the key topics covered in the report include:

Increasing use of unmanned systems

Unmanned systems are becoming increasingly useful, affordable and widely available, with applications in both public and private sectors. Law enforcement agencies across Europe are scaling up adoption of such systems, including drones and robots, to enhance situational awareness, improve safety and extend operational reach. These systems are employed for a range of tasks, such as monitoring, crime scene mapping, search and rescue operations, and the disposal of explosive ordnance, among others. Converging technologies present a significant opportunity for a breakthrough in the capabilities of unmanned systems.

Technical and regulatory challenges

The report highlights significant technical limitations and regulatory gaps that hinder the effective use of unmanned systems in law enforcement. Issues such as limited autonomy, dependence on industrial suppliers and the lack of clear guidelines for autonomous operations pose substantial challenges.

Security threats

Criminal and terrorist groups are rapidly adopting unmanned systems for illicit activities. The report warns of the potential for these systems to be used for criminal surveillance, smuggling and even attacks. The increasing accessibility and versatility of drones, in particular, present serious security concerns.

Public trust and regulation

Public trust is crucial for the legitimacy of law enforcement capabilities. The report emphasises the need for transparency, accountability and public engagement in the deployment of unmanned systems. Current regulations, while advancing, still have gaps, particularly in addressing non-compliant or criminal use.

Future operating environment

The future of law enforcement will require policing in a three-dimensional space, as unmanned systems operate in the air and on the ground, as well as on and under water. This shift will necessitate new strategies, technologies and training for law enforcement agencies.

Recommendations

The report provides a set of recommendations for European law enforcement agencies, including the development of a strategic direction, the establishment of a competency hub and the integration of unmanned systems into existing information systems. It also calls for investments in training, education and public trust-building initiatives.

Camect + Eagle Eye: Supercharging 911 Camera Sharing Across Texas

Across Texas, cities are embracing a smarter, faster, and more connected approach to public safety through real-time camera-sharing initiatives like Connect Dallas, Connect Arlington, and others. But what happens if a camera can't connect, or has too many false alerts?

Camect is a camera agnostic solution that bridges the gap between any camera and any Real-Time Crime Center (RTCC).

Camect acts as a universal gateway, connecting video monitoring systems—regardless of brand or type—to local law enforcement in a secure and efficient way.

Camect uses advanced AI to eliminate false alerts—no more wasted time on wind-blown branches or passing pets. Only true events of interest are captured and flagged. When an incident occurs, Camect makes it effortless to share specific video clips with authorities or stakeholders—instantly and securely—from anywhere, enabling faster decisions and more effective emergency response.

When paired with Eagle Eye Networks' 911 Camera Sharing technology, the impact is even greater. Eagle Eye connects directly to 911 dispatch centers via RapidSOS providing dispatchers with real-time visuals of the emergency scene as it unfolds, allowing them to relay accurate, actionable information to responding officers—everything from suspect descriptions to direction of flight. It enhances safety not just for the public, but for first responders, too.

Together, Camect and Eagle Eye form a proactive shield against crime, turning passive security systems into smart, collaborative tools for community protection. In business districts and residential neighborhoods alike, this tech-enabled approach ensures Texas cities stay one step ahead—making our communities safer, smarter, and better connected.

Armis Secures Italy's Primary Public Healthcare Provider for the City of Naples

Armis, the cyber exposure management & security company, today announced that ASL Napoli 1 Centro, Italy's primary public healthcare provider for the City of Naples, is securing its attack surface using Armis Centrix™, the Armis Cyber Exposure Management Platform.

Prior to working with Armis, ASL Napoli 1 Centro did not have the tools or capabilities to monitor physical and virtual assets in real time, which posed a challenge for its security and compliance. Armis Centrix™ was deployed with a clear goal: to provide ASL Napoli 1 Centro with a comprehensive, real-time view of its connected biomedical inventory and the associated risks to the overall environment.

Armis Centrix™ delivered detailed data right away, providing an accurate, real-time mapping of the organization's network-connected devices within the first month. The platform not only identifies devices, but it also determines whether a device is active or idle, vulnerable or patchable, consistently or intermittently connected, and whether it generates anomalous traffic.

ASL Napoli 1 Centro now monitors over 2,000 assets, with detailed insights on security posture, operational status, and actual usage, which has enhanced overall security for the organization and supported compliance initiatives.

ASL Napoli 1 Centro's network paints a picture of the physically dispersed, yet ever-connected nature of healthcare. Its network spans more than 100 facilities and encompasses roughly 18,000 biomedical devices, over 2,000 of which are connected and continuously collecting, processing and transmitting critical clinical data. With the help of Armis, ASL Napoli 1 Centro has improved its overall security posture and enabled compliance with national guidelines and NIS2 directives, supporting the delivery and continuity of patient care.

Eviden selected by the European Cybersecurity Competence Center and Network

Eviden, the Atos Group product brand leading in advanced computing, cybersecurity products, mission-critical systems and vision AI, today announced that it has won a call for projects from the European Cybersecurity Competence Center and Network (ECCC)[1] to improve the cyber protection and resilience of European critical infrastructures.

This ECCC initiative aims to develop a strong and coherent community around cybersecurity issues by strengthening collaboration, knowledge sharing and the deployment of innovative cybersecurity solutions on a European scale.

The CIPHER[2] (Cybersecurity Intelligence, Protection and Holistic Enterprise Resilience) consortium will directly contribute to the ECCC's mission to strengthen Europe's digital resilience by providing a standardized, collaborative facility for testing, validating, and certifying the cybersecurity posture of essential service operators.

Led by Eviden, CIPHER brings together 13 partners from 7 European countries — including critical infrastructure operators, research organizations, and cybersecurity SMEs — ensuring a strong, multi-sectoral approach to advancing Europe's cyber resilience.

Eviden's experience in applied cybersecurity on mission-critical systems, including its radio communications expertise, supports ECCC's objective to increase the European Union's cybersecurity capabilities, particularly in the context of the NIS2 directive (Network and Information Security 2).

Halcyon Joins CISA's Joint Cyber Defense Collaborative to Advance National Ransomware Resilience

Halcyon, the leading anti-ransomware solution provider, announced it has joined the Cybersecurity and Infrastructure Security Agency's (CISA) Joint Cyber Defense Collaborative (JCDC).

Halcyon's membership in JCDC emphasizes its ongoing commitment to strengthen collective defenses, advance ransomware resilience, and support joint operations that protect critical infrastructure and organizations across the United States.

Established in 2021, JCDC was created to bring together public and private sector partners to enable persistent, trusted collaboration against urgent cyber risks and to drive long term, proactive defense planning. As a member, Halcyon will contribute its ransomware expertise, share intelligence with government and industry peers, and participate in operational activities aimed at disrupting active ransomware campaigns.

"We are absolutely thrilled to welcome Halcyon to the JCDC. Private sector participation strengthens our collective defense against the ever-evolving threat of ransomware. The JCDC is at the heart of CISA's operational collaboration, and by incorporating key members like Halcyon and others, we can more effectively unify cyber operations across government, industry, and international organizations. Together, we are working tirelessly to secure our critical infrastructure and ensure the safety of all Americans." — Nick Andersen, Executive Assistant Director for Cybersecurity, CISA

"During my time in government, I saw firsthand how vital industry intelligence shared through JCDC was to defend networks and disrupt adversaries. So, when I joined Halcyon and saw the depth of our ransomware intelligence, it was immediately clear we needed to bring our intel into JCDC to strengthen the broader fight. Ransomware remains one of the most urgent national security and economic threats we face." — Cynthia Kaiser, Senior Vice President, Halcyon Ransomware Research Center

Censys and Rilian Technologies Partner to Strengthen Cyber Defense and Critical Infrastructure Security Across the Middle East

Censys, the authority for Internet intelligence and insights, has announced a strategic partnership with Rilian Technologies, a leading provider of AI-native cyber defense solutions for sovereign nations and critical infrastructure.

The partnership builds on Censys' rapid growth in the Middle East, where it supports national cybersecurity authorities, energy operators, financial institutions, technology organizations, and users across nearly every country in the region.

The partnership between Censys and Rilian Technologies supports Rilian's mission to protect sovereign nations and critical infrastructure by expanding access to Censys' Internet and ICS/OT intelligence across the Middle East. This ensures that government and commercial organizations can leverage the most comprehensive and authoritative view of the Internet for national-level detection, risk prioritization, and operational decision-making.

"Censys provides unmatched Internet intelligence and ICS/OT visibility, capabilities essential for defending national infrastructures from modern cyber threats," said Christian Schnedler, CEO of Rilian Technologies. "Through this partnership, Rilian will help bring Censys' unmatched insights directly to the government and commercial organizations that need them most to defend sovereign infrastructure and critical industries."

"Cybersecurity in the Middle East demands accurate, high-fidelity intelligence to protect critical infrastructure from increasingly sophisticated threats," said Sarah Ashburn, Chief Revenue Officer at Censys. "Our partnership with Rilian ensures that defenders across the region have the most comprehensive and up-to-date intelligence they need for national-level detection, prioritization, and response."

Indra Group is to manage the ticketing and access control systems across London's Public Transportation network

Indra Group has won one of the largest contracts in its history. Transport for London (TfL) has awarded the company the project to operate the ticketing and access control system of the entire public transportation network of London and its metropolitan area, the most advanced, innovative and trailblazing system in the western world

After an almost two-year transition period, Indra will become the sole provider of the ticketing system of a network encompassing more than 8,500 buses, nearly 400 metro stations and almost 300 other Overground, DLR, Elizabeth Line and suburban rail services

The project covers the operation, maintenance and evolution of a wide range of systems which Indra has over 30 years of proven experience as a benchmark technology provider of innovative urban public transportation solutions. Its track record includes complex environments involving multiple operators and different levels of management.

The systems it will manage include the turnstiles, validators, ticket vending machines, retail sales terminals and portable inspection equipment, as well as the entire technological infrastructure and an advanced back office integrating key cybersecurity functions, data management, reporting and coordination with third parties.

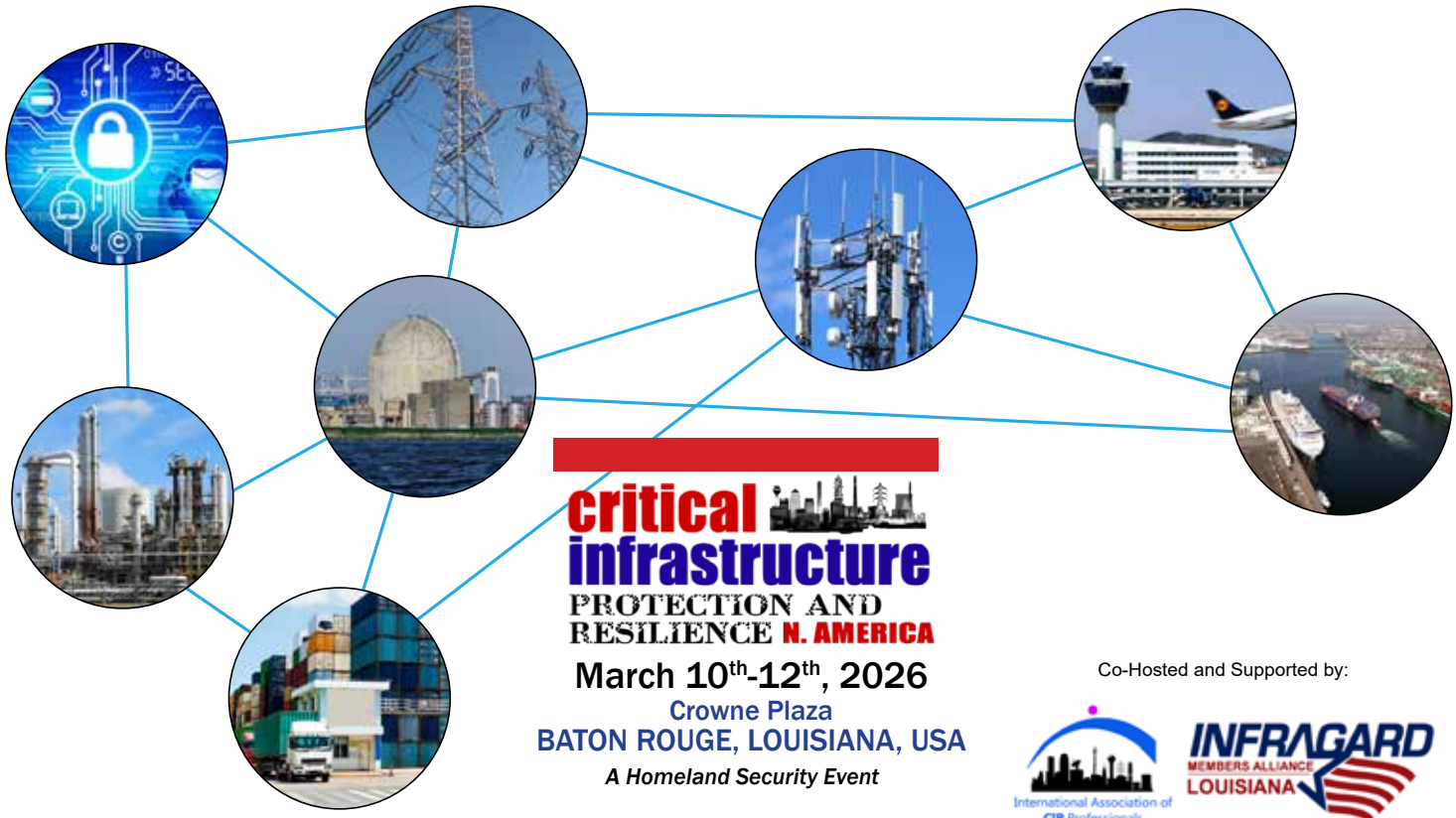
The project also envisages, in partnership with TfL, the implementation of new technologies to develop the system, make it more efficient and automate key processes; in short, to jointly create the next generation of the ticketing system for London.

critical infrastructure PROTECTION AND RESILIENCE EUROPE

ADVERTISING SALES

Bruce Bassin
Americas
E: bruceb@torchmarketing.co.uk
T: +1-702.600.4651

Paul Gloc
Rest of World
E: paulg@torchmarketing.co.uk
T: +44 (0) 7786 270820



critical infrastructure PROTECTION AND RESILIENCE N. AMERICA

March 10th-12th, 2026

Crowne Plaza
BATON ROUGE, LOUISIANA, USA

A Homeland Security Event

Co-Hosted and Supported by:

International Association of CIP Professionals

INFRAGARD MEMBERS ALLIANCE LOUISIANA

REGISTER ONLINE TODAY

Securing the Inter-Connected Society

Early Bird deadline - February 10th, 2026

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.

The 8th Critical Infrastructure Protection and Resilience North America brings together leading stakeholders from industry, operators, agencies and governments to debate and collaborate on securing America's critical infrastructure.

The last few years have seen the world immersed in a period with significant challenges and a great deal of uncertainty, which has stressed how important collaboration in protection of critical infrastructure is for a country's national security.

If you are responsible or involved in your planning and preparatoin for securing and protecting your critical assets and entities then join us for the next gathering of operators, government establishments and industry tasked with the region's Critical Infrastructure Protection and Resilience.

For further details and to register visit **www.ciprna-expo.com**

The premier discussion for securing America's critical infrastructure

CONFIRMED SPEAKERS INCLUDE:

Keynote: Colonel Robert P. Hodges, Deputy Secretary of Public Safety Services, Louisiana State Police

Keynote: Clay Rives, Director, Mayor's Office of Homeland Security and Emergency Preparedness, Baton Rouge

Keynote: Brian Harrell, Former Assistant Secretary for Infrastructure Protection, DHS

Mike Roskind, PNT Program Manager, Cybersecurity & Infrastructure Security Agency (CISA)

Charles Burton, Technology Director, Calcasieu Parish

Josie Ross, Emergency Management Officer, City of Henderson Department of Emergency Management

Joseph Threat, Chief Resilience Officer and Chief Administrative Officer, City of New Orleans

Dr. Brenda Connor, Senior Technical Managing Director, TTU Critical Infrastructure Security Institute

Det Sgt Kirsty Rigg, Counter Weapons Threat Team Lead, National Counter Terrorism Security Office UK

See **www.ciprna-expo.com** for more.

Global Cybersecurity Partner:

eset Cybersecurity Progress. Protected.

Supporting Organisations:

INFRAGARD MEMBERS ALLIANCE HOUSTON · AUTO-ISAC · GBRIA · MARNE SAFE 811 · CAMO · IACI · IT ISAC · Food Ag ISAC