critical infrastructure PROTECTION AND RESILIENCE NEWS

Official Magazine of

International Association of CIP Professionals

AUTUMN 2024
www.cip-association.org

FEATURE:
Artificial Intelligence Perspective: Goal Three of the CISA Roadmap

FEATURE:
Improving Interoperability for EU Joint Civil Protection Actions

FEATURE:
Navigating cybersecurity investments in the time of NIS 2

CISA LAUNCHES 2025/26 INTERNATIONAL STRATEGIC PLAN

critical infrastructure
PROTECTION AND RESILIENCE N. AMERICA

March 11th-13th, 2025
HOUSTON, TEXAS, USA
A Homeland Security Event

Are you sure your national infrastructure is secure?

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

Invitation to Attend

Register online today and save with Early Bird Discounts

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

The Biden Administration rolled out a new critical infrastructure memorandum, titled National Security Memorandum on Critical Infrastructure Security and Resilience (NSM-22) which is intended to set forth the role of the federal government, including responsibilities for specific federal agencies, in protecting U.S. critical infrastructure.

NSM-22 serves to supplant PPD-21, formally known as the Presidential Policy Directive – Critical Infrastructure Security and Resilience (pdf). PPD-21, a memorandum issued during the Obama Administration, designated 16 critical infrastructure sectors that will be subject to additional oversight through the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).

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

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

Register today for Early Bird Savings on delegate fees.

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

The premier discussion for securing America's critical infrastructure

Co-Hosted by:

International Association of CIP Professionals
INFRAGARD MEMBERS ALLIANCE HOUSTON

Speakers include:

- David Carroll, Associate Director for Mission Engineering, CISA
- Brannan Villee, Strategic Program Manager, Department of Homeland Security, Science & Technology Directorate
- Norman Speicher, Program Manager, Department of Homeland Security, Science and Technology Directorate
- Faye Francy, Executive Director, Automotive Information Sharing and Analysis Center (Auto-ISAC)
- Clint Ladd, Critical Infrastructure Protection Coordinator, Texas Department of Public Safety / Texas Office of Homeland Security
- Annie Hunziker Boyer, Chief, Chemical Security Policy, Rulemaking, and Engagement Branch, CISA
- Marco Ayala, President, Houston InfraGard Members Alliance
- Lt. Col. Tommy Waller, USMC Ret., President & CEO, Center for Security Policy, USA

For full speaker line up visit www.ciprna-expo.com/speakers2025

To discuss exhibiting and sponsorship opportunities contact:

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 270 820

Supporting Organisations:

International Association of CIP Professionals · INFRAGARD MEMBERS ALLIANCE LOUISIANA · Help2Protect · STIME · ISIO - International Security Industry Organization

Executive Sponsors:

TIA · AUTO-ISAC · INSTITUTE FOR HOMELAND SECURITY

Flagship Media Partner:

critical infrastructure PROTECTION AND RESILIENCE NEWS

KEEPING THE CONVERSATION, AND COLLABORATION, GOING

November saw the timing come together for 'CIP Week in Europe' and Critical Infrastructure Protection Month in North America, both with the goal of highlighting the need for operator/owners of critical infrastructure, research institutes, agencies and their supporting government departments and law enforcement to be vigilant against the broad range of threats we are facing.

As the threat from cyber attacks, whether state sponsored, or organised criminal groups, continues to grow, and we see much resource being funneled towards cyber security, we must not forget the danger of physical threats from the likes of terrorism, man-made or natural disasters.

CIP Week in Europe, in Madrid, saw many European nations represented, as well as further afield from North America, the Middle East and Asia, and delivered a broad range of interesting discussions and interactive workshops, all designed to educate, inform and expand your network, ideas and strategies for securing your CI. Read our review about CIP Week in Europe later in this issue.

We live in a more precarious world, so the need for sharing of ideas and collaboration on programs and initiatives is greater than ever. In this issue, we see what CISA has in store for its International Strategic Plan for 2025/26, reinforcing the need to strengthen the security and resilience of foreign assets to help protect assets both home and abroad.

Collaboration and the sharing of ideas and information is key to making a more secure society. Let's keep the conversations going.

Enjoy reading this issue, we hope you once again find it interesting and informative.

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.

FY2025-2026 CISA International Strategic Plan

The Cybersecurity & Infrastructure Security Agency (CISA) published their 2025-2026 International Strategic Plan with a commitment to reducing risk to the globally interconnected and interdependent cyber and physical infrastructure.

In today's interdependent and interconnected world, the protection and security of our cyber and physical infrastructure requires the concerted efforts of public and private partners around the globe. The Cybersecurity and Infrastructure Security Agency (CISA) is a globally recognized leader in shaping and implementing proactive approaches to reduce risk and increase the resilience of critical infrastructure on which the United States (U.S.) and its partners depend.

To effectively marshal its resources and guide operations, CISA issued the 2023-2025 CISA Strategic Plan, the agency's first comprehensive strategic plan since CISA's establishment in 2018. In recognition of the reality that today's threats do not respect borders, CISA developed this CISA International Strategic Plan as a complementary guide for CISA's international activities and outcomes.

This CISA International Strategic Plan acknowledges that the risks we face are complex and geographically dispersed, and that we cannot achieve our objectives in a vacuum. It is imperative that we expand visibility into internationally shared systemic risks. The maturity and security practices of global owners and operators of both cyber and physical infrastructure, technology, supply chains, and systems vary widely. Sharing timely, relevant, and accurate threat information and risk reduction advice with international partners provides the foundation for a more secure cyber-physical environment for all of us.

The CISA International Strategic Plan goals are to:

1. Bolster the Resilience of Foreign Infrastructure on Which the U.S. Depends.

2. Strengthen Integrated Cyber Defense.

3. Unify Agency Coordination of International Activities.

Through the goals and objectives outlined in this CISA International Strategic Plan – in coordination with the Department of Homeland Security (DHS), the Department of State, and partners across the interagency, and in accordance with U.S. national security, economic, and foreign policy priorities – CISA will assess and prioritize critical infrastructure dependencies and partner with foreign entities to advance CISA's homeland security mission.

Strategic Intent

The CISA International Strategic Plan will focus and guide the agency's international efforts over the 2025–2026 period. It highlights the agency's commitment to reducing risk to the globally interconnected and interdependent cyber and physical infrastructure that Americans rely

on every day. Our aim is to shape the international environment to reduce risk to critical dependencies and set conditions for success in cooperation, competition, and conflict. The CISA International Strategic Plan lays out three goals CISA must achieve to address the ever-changing and dynamic challenges facing America and our international partners. The first two goals focus on "what" the agency will work on in the international environment to achieve our "why" – 1) to reduce risk to and build resilience of foreign assets, systems, and networks that impact U.S. critical infrastructure, 2) understand shared global threats to critical infrastructure, and 3) support collective defense. The third goal focuses internally to promote unified action, working as One CISA to conduct international activities.

Strategic Approach

The approach laid out in this CISA International Strategic Plan aligns with guidance set forth in the National Security Strategy, National Cybersecurity Strategy, U.S. International Cyberspace and Digital Policy Strategy, CISA Strategic Plan 2023–2025, CISA Stakeholder Engagement Strategic Plan FY2023-2025, and CISA Cybersecurity Strategic Plan 2024–2026, as well as the identified priorities of the Secretary of Homeland Security. The CISA International Strategic Plan and the U.S. International Cyberspace and Digital Policy Strategy firmly align to bolster and broaden international alliances to mature cyber defense efforts, both domestically and internationally. This involves fostering collaborative relationships with global partners; sharing expertise, technical resources, and best practices; and collectively fortifying cyber resilience to address emerging threats in an interconnected world. Our strategic approach will not only advance the resilience of critical infrastructure dependencies at home and abroad, but it will also ensure a long-term commitment in strengthening international partnerships that are essential for CISA's mission success. As part of coordinated U.S. government efforts, CISA will proactively engage and support international partners to assess, influence, and assist with reducing risk and strengthen the security and resilience of foreign assets,

systems, and networks on which our nation's critical infrastructure depends. As threats evolve across the spectrum of competition with state and non-state actors, no single organization or entity has all the answers for how to address cyber and physical threats to critical infrastructure. Therefore, CISA will prioritize operational collaboration and international activities to achieve mutual interests and goals with our partners. This plan centralizes CISA's focus and coordination on goals and objectives that increase homeland and national security. More importantly, it positions CISA to support the internal coordination of international activities through the execution of annual planning cycles. This CISA International Strategic Plan seeks to streamline or eliminate overlapping and redundant systems to synchronize complex international issues that cut across our agency.

Overall, our aim is to build, strengthen, and sustain international relationships to:

1. Advance homeland and national security objectives.
2. Prevent incidents and increase resilience of physical and cyber critical infrastructure at home and abroad.
3. Increase awareness to detect, deter, and disrupt emerging threats and hazards.
4. Manage and reduce systemic risks.
5. Increase understanding of international critical infrastructure interdependencies and anticipate cascading impacts.
6. Influence international policy, standards, and best practices.
7. Assist key partners to address their capability shortfalls.
8. Expand bilateral/multilateral exchanges of expertise, in tandem with increased federal inter- and intra-agency coordination, to improve risk management and incident response capacity.
9. Mature and strengthen CISA's international partnerships, arrangements, and policies.

Goal 1: Bolster the Resilience of Foreign Infrastructure on Which the U.S. Depends

Interconnected Critical Infrastructure Graphic

Recognizing that much of U.S. critical infrastructure interconnects and/or is interdependent with foreign assets, systems, or networks, CISA will work closely with domestic and international partners to bolster the security and resilience of the international critical infrastructure on which the U.S. depends. These interconnections and interdependencies span the full range of critical infrastructure sectors: pipelines, telecommunications, and essential supply chains, among others. Malicious cyber actors continue to exploit vulnerabilities across these sectors to target critical infrastructure through ransomware and other cyberattacks. The threat from global terrorism remains a persistent concern and a significant threat to U.S. and international facilities. Thus, it is essential for CISA to work with partners to assess and reduce risk from foreign critical dependencies impacting U.S. critical infrastructure resilience. In doing so, CISA must strengthen exchanges with international partners that promote our priorities abroad as well as influence standards, regulations, and policies to advance homeland and national security objectives. A collaborative approach to understanding interconnected critical infrastructure systems will set conditions for the U.S. and our international partners to proactively develop strategies, policies, and programs that integrate risk reduction efforts and reflect mutual and multi-stakeholder security interests at home and abroad.

1.1. Identify and prioritize foreign critical infrastructure on which the nation depends and bolster its security and resilience.

The U.S. depends on foreign-owned systems that support our critical infrastructure sectors such as communications, transportation, information technology, energy, financial services, and critical manufacturing. CISA will work with interagency and international partners to identify and understand which international systems and assets are truly critical to the nation's critical infrastructure and assess how they are vulnerable to create strategies to manage shared risks. CISA will also work with interagency and international partners to promote a shared understanding of global threats to critical infrastructure security and resilience, such as cyberattacks, chemical and improvised explosive devices, threats to supply chain interdependencies, foreign malign investments, and climate change. Managing risk and bolstering resilience will require long-term, strategic collaboration between public and private sectors at home and abroad.

Enabling Measure: In coordination with the Department of State and relevant U.S. government partners, we will broaden our understanding of systemic risk by expanding our visibility into infrastructure and supply chain vulnerabilities for priority foreign critical infrastructure upon which the U.S. depends.

Measure of Effectiveness:

1. Increase the number of U.S. government activities coordinated by CISA to advance the security and resilience of prioritized foreign critical infrastructure and supply chains.
2. Increase the number of global partner actions taken to address risks to prioritized foreign critical infrastructure.
3. Increase the number of domestic partner actions taken to mitigate potential disruptions of U.S. critical infrastructure operations resulting from dependencies with foreign assets, systems, and supply chains.

1.2. Strengthen international partnerships that promote U.S. critical infrastructure priorities and interests abroad.

CISA seeks to expand visibility into internationally shared threats and systemic risks. To improve situational awareness for both CISA and our international stakeholders, we must mature multidirectional communications with external partners, including timely incident reporting and the systematic sharing of threat and vulnerability information. Strengthening includes accelerating the speed, improving the accuracy, and enabling the effectiveness of critical information sharing, while using CISA as a hub for multi-stakeholder initiatives. We will use CISA's cross-functional expertise to foster communication and information sharing with global partners at scale, which will advance the resiliency of our critical infrastructure against shared challenges and preserve our ability to communicate in the event of an emergency. This will create a foundation for advancing international efforts that mature our collective ability to plan for, detect, deter, and disrupt emerging threats and hazards to cyber and physical infrastructure and interoperable emergency communications. Deepening the understanding of shared and systemic risk with our partners will strengthen the protection and resilience of critical infrastructure on which the nation relies.

Enabling Measure: We will expand our ability to execute joint operational activities, capacity development efforts, and shared policy frameworks that advance U.S. priorities for defending cyberspace and protecting U.S. critical infrastructure.

Measure of Effectiveness:

1. Increase the number of joint operational activities conducted with global partners to build public and private capacity to deter, prevent, protect, and respond to incidents to critical infrastructure.
2. Increase information sharing exchanges with global partners to promote U.S. security and resilience priorities and to

enhance CISA's programs, services, and products.

1.3. Shape operational and technical global standards, regulations, policies, guidelines, and best practices to advance security.

CISA will work with interagency partners to support standards activities—in coordination with the DHS Science and Technology Directorate—through standard development organizations that can advance U.S. interests. Within CISA's authorities, our aim is to promote and support a wide array of portfolios, including but not limited to cyber and physical critical infrastructure, emerging technology, chemical security, emergency communications, school safety, bombing prevention, and more to ensure that systems, infrastructure, government, business, and the public can withstand and recover from deliberate attacks, accidents, and natural hazards. Where appropriate, we will advance and contribute to the development and adoption of operational and technical international standards and regulations to strengthen cybersecurity, fortify critical infrastructure security and resilience, and improve emergency communication. CISA holds a shared approach to international standards, regulations, guidelines, and best practices for critical infrastructure security and critical emerging technologies, to include artificial intelligence (AI). This will help accelerate standards that contribute to interoperability and promote U.S. competitiveness and innovation with our partners.

Enabling Measure:

1. We will advance open, transparent, and rules-based standards processes to ensure that globally relevant standards meet U.S. national security requirements for critical infrastructure.

2. We will work with partners to counter the influence of adversaries attempting to unduly shape standards in a manner which would represent a threat to national security.

Measure of Effectiveness:

1. In coordination with government, industry, and academic partners, increase the development and publication of technical standards for adoption by international standards and policy setting bodies that advance the protection, interoperability, and resilience of U.S. critical infrastructure.

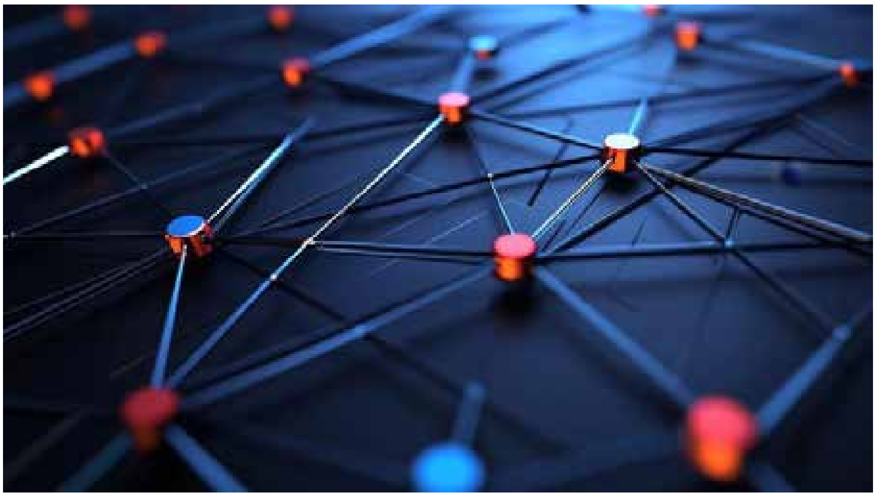
Goal 2: Strengthen Integrated Cyber Defense

Integrated Cyber Defense graphic

Cybersecurity threats extend beyond national borders. Strong international cyber defense partnerships set conditions that reduce risk and minimize the impact of attempts to infiltrate, exploit, disrupt, or destroy critical infrastructure systems that support our national critical functions (NCFs). Engaging international partners allows CISA to build trust, illuminate threats, and facilitate the free flow of cybersecurity defense information. We will work with partners, international organizations, and nongovernmental organizations to influence global cybersecurity practices and standards that promulgate cyber safety and security at scale. Bolstering the capabilities of key partners improves our collective cyber defense abroad against state and non-state actors.

2.1. Enable cyber defense with partners to reduce collective risk.

International partners contribute essential information to support CISA's cybersecurity mission. A network of trusted partners provides increased visibility into—and ability to mitigate—cybersecurity threats, vulnerabilities, and campaigns. Our aim is to increase and mature our network of trusted partners through our bilateral and multilateral Computer Security Incident Response Team (CSIRT)-CSIRT engagements. Through these engagements, we seek to strengthen CSIRT-CSIRT



relationships that enable the exchange of actionable operational information, which includes product sharing, vulnerability alerts, victim notifications, tactics, techniques, and procedures as well as evaluating unique international inputs to reduce risk. This effort will facilitate a collective response and provide a vehicle for partners to share information that builds trust and global cyber situational awareness—especially for those foreign systems, networks, and assets truly vital to the nation's critical infrastructure. We will strive to set an example as the premier CSIRT organization and work with international partners to understand how incidents occur, how to prevent them, and to provide technical resources that alleviate critical operational gaps. Beyond immediate threat information, these operational partnerships help inform international exercises that will enable us to better understand risks and provide additional ways and means to better manage threats and risk abroad.

Enabling Measure: We will increase trust and strengthen operational collaboration through bilateral and multilateral engagements with international partners by expanding participation in CSIRT-CSIRT engagements.

Measure of Effectiveness:

1. Increase the number of trusted international CSIRT partners.

2. Increase the percent of bilateral and multilateral CSIRT engagements that reduce combined risk.

3. Increase the number of CSIRT partners that apply recommended risk mitigations prior to exploitation.

2.2. Drive standards and security at scale to increase cyber safety.

For decades, the U.S. has worked through international institutions to define and advance responsible state behavior in cyberspace, steering partners toward developing secure technology from inception. As part of the broader national effort, CISA will encourage international partners to define, adopt, and implement global cybersecurity standards, norms, and best practices that promote U.S. cybersecurity interests.
The agency will also provide guidance, advice, and expertise to help define and implement safe global standards, norms, and best practices that support U.S. domestic cybersecurity interests. Our aim is to set the bar high for global standards and prioritize them to reflect CISA interests and implement them as a critical element to protect citizens. As some of the most visible examples, CISA's international focus is to encourage the widespread adoption of Secure by Design practices, including adoption of software bills of materials, secure AI systems, open-source security, and coordinated vulnerability disclosures.

Enabling Measure: In collaboration with international public and private sector partners, we will advance a global commitment to safe and secure software development and deployment.

Measure of Effectiveness:

1. Increase in international standards that recommend frameworks for secure software development at the onset of the software development lifecycle.

2. Increase the number of partner states, international organizations, and industries that adopt and implement the principles of Secure by Design.

2.3. Increase cyber and physical resilience capabilities of key partners.

The breadth and depth of the international cybersecurity challenge exceeds the capacity of any one organization. It is paramount that key partners possess the fundamental capabilities to safeguard and defend their connected critical infrastructure that impact our NCFs. Our aim is to establish an environment where our partners can organically detect threats, assess potential impacts, and receive and exchange real-time risk reduction actions that increase collective security and resilience and support the rapid establishment of consistent, secure, and effective interoperable emergency communications. CISA possesses capabilities that can uniquely contribute to homeland and national security objectives—especially as part of larger U.S. government efforts to improve the cybersecurity capabilities of priority international partners. As the U.S. strengthens relationships with key partners, CISA can provide training, exercises, and information sharing capabilities. These activities can assist international partners in developing and growing organic risk reduction capabilities, while setting supporting priorities for the investment and divestment of limited resources to fill collective capability shortfalls.

Enabling Measure: In collaboration with the Department of State, we will advance shared cybersecurity priorities and strengthen international partner capacity to support these priorities through the focused delivery of CISA services that proactively and collaboratively bolster our international cybersecurity and resilience.

Measure of Effectiveness:

1. Increase the number of CISA services delivered to international partners that address identified security and resilience gaps.

2. Increase in the percent of program participants equipped with required competencies in cyber or physical security and resilience.

3. Expand the network of foreign train-the-trainer partners capable and approved to provide CISA-based training within their regions.

4. Increase the percent of partners reporting strengthened capabilities to manage their own risk.

Goal 3: Unify Agency Coordination of International Activities

Connecting lines

An effective international plan depends on unity of effort across the agency's divisions and mission enabling offices (offices). Accomplishing unity of effort will require that CISA internally prioritizes, coordinates, deconflicts, and aligns international activities through improved organization and governance, integrated functions, and a well-trained workforce.

3.1. Strengthen and institutionalize CISA's governance of international activities.

The CISA Stakeholder Engagement Division (SED) will establish a governance structure to advise on international matters and provide a clear articulation of the agency's international priorities. Taking into account inputs from divisions and offices, these priorities will provide clear guidance that is consistent with CISA's authorities and domestic requirements as well as broader DHS and national security policies.

Enabling Measure: We will establish internal agency processes and procedures for governing the agency's international activities using the One CISA approach.

Measure of Effectiveness:

1. Increase the number of governance documents and processes that improve standardization and transparency of agency international activities.

3.2. Align and synchronize CISA's international functions, capabilities, and resources.

CISA will support systematic information sharing across the agency through policy coordination and the collection and dissemination of international lessons learned to effectively realize the full range of specialized expertise and capabilities across the agency. SED will coordinate CISA's international communications and activities across CISA to provide the agency with situational awareness of current and projected international activities. This coordination will address gaps and eliminate duplication of effort while ensuring timely execution of operational priorities and alignment of CISA's international activities with this strategic plan and national security priorities.

Enabling Measure: We will optimize internal business operations to ensure the coordinated delivery of products and services to international partners that effectively advance cyberspace defense and U.S. critical infrastructure security and resilience.

Measure of Effectiveness:

1. Increase the percent of cross-cutting activities coordinated through CISA International Affairs.
2. Increase in internal products and services that improve widespread awareness of key international cybersecurity and critical infrastructure security and resilience issues.

3.3. Equip CISA's workforce through training and education to promote CISA's capabilities on the global stage.

With an inherent domestic focus, we recognize that there are skills CISA needs to provide the workforce to influence the international system. CISA will develop and provide training opportunities for employees who will deploy overseas as well as those engaged in deliberate international activities. SED will aim to facilitate DHS and State Department pre-deployment training for Attachés, Liaison Officers, and Technical Advisors deploying overseas, including a CISA familiarization program to ensure a baseline understanding of CISA's organization, role, responsibilities, authorities, and strategic objectives. SED will provide international affairs etiquette guidance to all travelers as part of the travel preparation process. For CISA leadership and travelers conducting potentially sensitive engagements, SED will provide a tailored pre-departure briefing encompassing cultural norms and U.S. foreign policy goals with recommended talking points.

Enabling Measure: CISA, through its workforce, is prepared to actively and effectively engage in international efforts to advance cyberspace defense, safe and secure technology development and deployment, and critical infrastructure security and resilience.

Measure of Effectiveness:

1. Increase the percent of CISA personnel trained and provided with resources to deliver international services.
2. Increase in the percent of CISA personnel who report that specialized training improved their capability to represent the agency effectively while performing international activities.

Conclusion

Robust and trusted international partnerships serve as a force multiplier across the spectrum of global competition. Successful partnerships require commitment, dedication, and time to build trust. In coordination with DHS and the State Department, CISA will develop, strengthen, and sustain these relationships. This CISA International Strategic Plan provides a framework to build and maintain an agency posture with international partners to enable the U.S. to compete with and prevail against current and future threats. Importantly, this plan addresses multiple challenges under different conditions and creates the framework to prioritize agency efforts.

These goals position CISA strategically with a posture that reinforces critical partnerships abroad to overcome complex and interconnected challenges. The strategic approach aligns CISA with the broader U.S. government as well as our international partners to enable access, develop capacity, and ensure the flexibility to support national efforts to compete globally against state and non-state actors.

This CISA International Strategic Plan creates opportunities for shared success and is a process, not simply a publication; therefore, CISA will review progress quarterly. Unpredictability in the international security environment, or obstacles to our progress, may drive us to change course. We will remain agile and shift our focus to ensure we are integrating the right people, processes, technology, and partners at the right time, place, and space for mission success. Just as our threats and adversaries adapt to and shape the cyber and physical security environment, CISA will continue to evolve to fulfill the vision of a secure and resilient infrastructure for the American people—this CISA International Strategic Plan establishes a proactive path to achieve that vision.

Commission takes action to ensure complete and timely transposition of EU directives

The Commission is adopting a package of infringement decisions due to the absence of communication by Member States of measures taken to transpose EU directives into national law. The Commission is sending a letter of formal notice to those Member States who have failed to notify national measures transposing directives, whose transposition deadline expired recently. In this case, there are 26 Member States who have not yet notified full transposition measures for two EU directives in the field of digital economy and migration, home affairs and security union. Member States concerned now have two months to reply to the letters of formal notice and complete their transposition, or the Commission may decide to issue a reasoned opinion.

The Commission calls on 23 Member States to fully transpose the NIS2 Directive

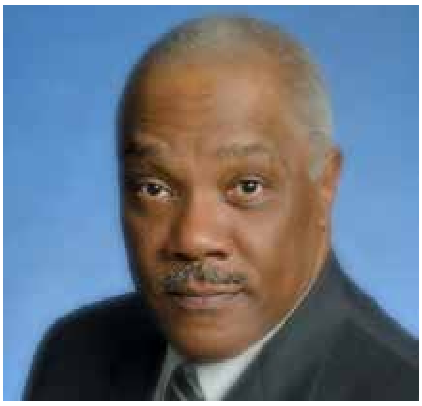
Today, the European Commission decided to open infringement procedures by sending a letter of formal notice to 23 Member States (Bulgaria, Czechia, Denmark, Germany, Estonia, Ireland, Greece, Spain, France, Cyprus, Latvia, Luxembourg, Hungary, Malta, Netherlands, Austria, Poland, Portugal, Romania, Slovenia, Slovakia, Finland and Sweden) for failing to fully transpose the NIS2 Directive (Directive 2022/2555). Member States had to transpose the NIS2 Directive into national law by 17 October 2024. The NIS2 Directive aims to ensure a high level of cybersecurity across the EU. It covers entities operating in critical sectors such as public electronic communications services, ICT service management, digital services, wastewater and waste management, space, health, energy, transport, manufacturing of critical products, postal and courier services, and public administration. Full implementation of the legislation is key to further improving the resilience and incident response capacities of public and private entities operating in these critical sectors and the EU as a whole. The Commission is therefore sending letters of formal notice to the other 23 Member States concerned that now have two months to respond and to complete their transposition and notify their measures to the Commission. In the absence of a satisfactory response, the Commission may decide to issue a reasoned opinion.

The Commission calls on Member States to transpose agreed rules ensuring the protection of critical infrastructure and resilience of critical entities

The European Commission decided to open infringement procedures by sending a letter of formal notice to 24 Member States for failing to notify national measures transposing the Directive (EU) 2022/2557 on the resilience of critical entities (CER Directive). Member States had to transpose the CER Directive by 17 October 2024. It repeals the Council Directive (2008/114/EC) on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. The new Directive shifts the approach from the protection of critical infrastructure to enhancing the resilience of the entities operating that infrastructure, while expanding the sectoral scope from 2 to 11 sectors. The Directive ensures the provision of vital services for our society and our economy in key sectors such as energy, transport, health, water, banking and digital infrastructure, by strengthening the resilience of critical infrastructure and critical entities against a range of threats, including natural hazards, terrorist attacks, insider threats, or sabotage. Belgium, Bulgaria, Czechia, Denmark, Germany, Greece, Spain, France, Croatia, Cyprus Latvia, Lithuania, Luxembourg, Hungary, Malta, the Netherlands, Austria, Poland, Portugal, Romania, Slovenia, Slovakia, Finland and Sweden have not communicated to the Commission any national measures transposing this Directive by the set deadline of 17 October 2024. The Commission is therefore sending letters of formal notice to the concerned Member States, which now have two months to respond, complete their transposition and notify their measures to the Commission. In the absence of a satisfactory response, the Commission may decide to issue a reasoned opinion.

Artificial Intelligence Perspective: Goal Three of the CISA Roadmap

The Cybersecurity Infrastructure Security Agency (CISA) released the CISA Roadmap for Artificial Intelligence 2023-2024 in 2023, soon after Executive Order 14110 was published. The roadmap aligned with the EO's Sections 4.3 and 11.0. Section 4.3 states explicitly that Executive Agencies will facilitate the management of AI in critical infrastructure and cybersecurity, while Section 11 directs the strengthening of American Leadership globally.



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

One key initiative is for the National Institute of Standards and Technology (NIST) to develop a companion resource to the AI Risk Management Framework, NIST AI 100-1, for generative AI (GAI). In July 2024, NIST released NIST AI 600-1 Artificial Intelligence Risk Management Framework for Generative Artificial Intelligence, focusing on managing risks unique to or exacerbated by GAI.

The CISA Roadmap provided five lines of effort for Artificial

Intelligence (AI) in cybersecurity and infrastructure security. These lines of effort promote the responsible use and protection of AI systems. The five lines of effort in the CISA Roadmap for Artificial Intelligence 2023-2024 are:

1. Responsibly Use AI to Support Our Mission.
2. Assure AI Systems.
3. Protect Critical Infrastructure from Malicious Use of AI.
4. Collaborate with and Communicate on Key AI Efforts.
5. Expand AI Expertise in Our Workforce.

This perspective will concentrate on the Line of Effort Three: Protect Critical Infrastructure from Malicious Use of AI.

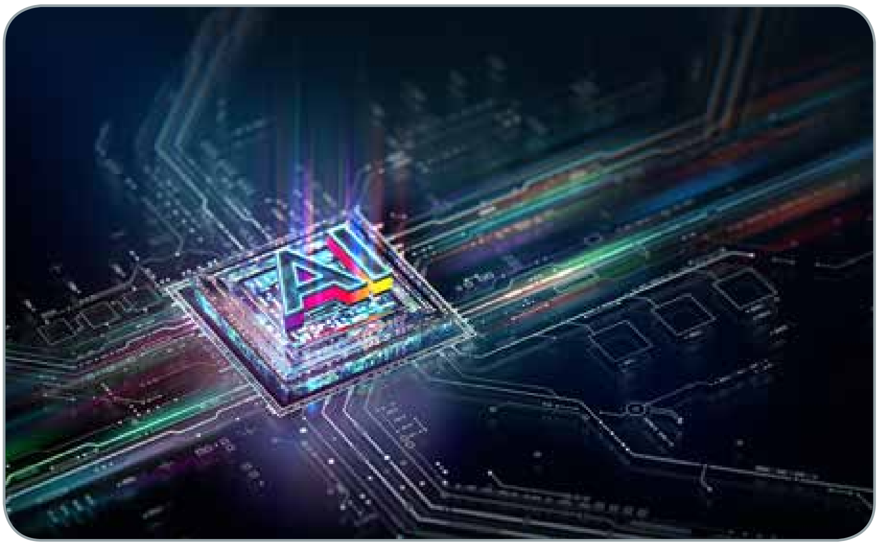
This effort is intended to assess and mitigate AI threats to the nation's critical infrastructure in collaboration with other government agencies and industry partners. It has two outcomes.

1. Engage stakeholders through tabletop exercises to protect AI systems from adversarial manipulation or abuse.
2. Advance AI risk management practices across the critical infrastructure community by publishing and disseminating decision support materials, such as a risk management guide for AI risks to critical infrastructure.

The approach is to track the number of publications and engagements that support shared awareness of emerging AI-related risks and advances in AI risk management practices.

There are three objectives.

1. Engage Industry Stakeholder Partners



2. Assess AI Risks to Critical Infrastructure
3. Use CISA Partnerships and Working Groups, including the Joint Cyber Defense Collaborative (JCDC AI).

In 2021, CISA created the Joint Cyber Defense Collaborative (JCDC) in partnership with industry and government to address cybersecurity challenges and threats. Associate Director Clayton Romans released a blog post in 2024 that discusses the JCDC 2024 priorities, which include defending against advanced persistent threat operations, raising the cybersecurity baseline, and anticipating emerging technology and risks.

The JCDC priorities for 2024 are:

1. Discover and defend against malicious abuse by APT actors, particularly those backed by the PRC, on and against U.S.-based infrastructure.
2. Prepare for major cyber incidents, including updating the National Cyber Incident Response Plan (NCIRP).
3. Help provide state and local election officials with information and tools to secure their networks and infrastructure against cyber threats.
4. To measurably decrease the impact of ransomware on critical infrastructure.
5. Make measurable progress toward a world where technology is Secure by Design.
6. Decrease the risk posed by AI to critical infrastructure.

The CISA Roadmap for Artificial Intelligence 2023-2024, released by the Cybersecurity Infrastructure Security Agency (CISA) following Executive Order 14110, outlines five key lines of effort to enhance AI use in cybersecurity and infrastructure security. These efforts include responsibly using AI, assuring AI systems, protecting critical infrastructure from malicious AI use, collaborating on AI initiatives, and expanding AI expertise within the workforce. The document emphasizes Line of Effort Three, which focuses on mitigating AI threats to critical infrastructure through stakeholder engagement and advancing AI risk management practices. The Joint Cyber Defense Collaborative (JCDC) supports

these initiatives with priorities such as defending against advanced persistent threats, preparing for cyber incidents, and reducing ransomware impact. The roadmap aims to ensure AI's safe, secure, and trustworthy development and use, reinforcing American leadership in global cybersecurity. This perspective is not a complete review of actions prompted by EO 14110. It does provide the reader with foundations for further review.

Dr. Ron Martin is a Professor of Practice at Capitol Technology University, specializing in the functional areas of Critical Infrastructure, Industrial Control System Security, Identity, credentials, and Access Management. Ron is an IEEE Senior Member, an active contributor at the Cloud Security Alliance, and a member of the International Association of CIP Professionals.

Critical Infrastructure Protection Week *in Europe*

International Association of CIP Professionals

14th-16th October 2025 - Brindisi, Italy

critical infrastructure
PROTECTION AND
RESILIENCE EUROPE

SAVE THE DATES

Securing the Inter-Connected Society

The International Association for CIP Professionals is delighted to be hosting the 2025 CIP Week in Europe with the patronage of the City of Brindisi.

The premier event for the critical infrastructure protection and resilience community, Critical Infrastructure Protection and Resilience Europe (CIPRE) brings together leading stakeholders from industry, operators, agencies and governments to collaborate on securing Europe.

CALL FOR PAPERS - Deadline 31st March 2025

The CIPRE Conference Committee are currently accepting abstracts for consideration for inclusion in the 2025 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 Brindisi, Italy for the next CIP Week in Europe and the 10th 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

With the patronage of the City of Brindisi

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

Improving Interoperability for EU Joint Civil Protection Actions

TIEMS team in the FIRE – RES EU project has developed an Opinion Paper on "Improving Interoperability for EU Joint Civil Protection Actions".

This Opinion Paper aims to initiate discussions to improve interoperability among EU Civil Protection organizations. By leveraging insights from the experience of TIEMS members, previous TIEMS projects, and initial findings from the FIRE-RES project, this presentation highlights the need for a comprehensive approach to enhancing coordination, communication, and collaboration across national borders in Europe.

Interoperability among EU Civil Protection organizations is essential for effective disaster response and resilience. The ability of different national systems to work together seamlessly ensures timely and coordinated efforts during emergencies, ultimately saving lives and resources. While each nation has developed its own protocols and structures, the growing frequency and complexity of cross-border emergencies necessitate a more integrated approach.

The EU Host Nation Support (HNS) guidelines provide a precedent for discussing command and control interoperability. These guidelines have established a framework for receiving and providing assistance during disasters, highlighting the importance of standardized procedures and cooperation among EU member states (UCP Knowledge Network). Similarly, this opinion paper advocates for a framework to enhance interoperability in civil protection, with a focus on command and control, leveraging insights from various EU Projects, TIEMS research and experience, and recent efforts such as FIRE-RES.

Objective: The primary objective of this opinion paper is to emphasize the need for a comprehensive roadmap to enhance command and control interoperability among EU Civil Protection organizations. While not a direct deliverable of the FIRE-RES project, the findings and experiences from FIRE-RES are highly applicable to this initiative and further support the previous research and projects by TIEMS. By identifying key issues and presenting relevant research and project findings, this paper aims to:

- Highlight the importance of interoperability in civil protection.
- Identify the challenges and opportunities related to interoperability.
- Propose the development of a detailed roadmap to address these challenges and leverage opportunities.

A next step would be the creation of a project under the EU framework that tackles interoperability through in-depth analysis and collaborative efforts, much like the development of the HNS guidelines. This approach would focus on the people, systems, and structures surrounding civil protection response, ensuring a robust and coordinated effort across the EU.

FIRE-RES

Improving Interoperability for EU Joint Civil Protection Actions

Toward Guidelines for Command and Control

By TIEMS Team in the FIRE- RES Project
Presented By
K. Harald Drager
TIEMS President
khdrager@online.no

Funded by the European Union

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101037419. It does not necessarily reflect the view of the European Union and in no way anticipates the Commission's future policy in this area.

Insights from FIRE-RES

Project Overview: The FIRE-RES project, funded under the European Union's Horizon 2020 research and innovation program, aims to develop innovative solutions for creating fire-resilient territories across Europe. The project addresses extreme wildfire events (EWEs), which pose significant environmental, economic, and social threats. FIRE-RES integrates research, technology, civil protection, policy, and governance to innovate processes, methods, and tools for effective fire management.

Key Findings: The insights from the FIRE-RES project highlight several critical aspects that are relevant to developing command and control interoperability within EU Civil Protection systems:

- Multi-Actor Collaboration: Effective disaster management requires collaboration among multiple actors across different levels and sectors. FIRE-RES demonstrated the importance of engaging diverse stakeholders in planning and implementing fire management strategies. This involves fostering partnerships between public and private entities, enhancing the role of local communities, and ensuring that all relevant actors are equipped with the necessary knowledge and resources. Translating this to command and control interoperability, it is essential to establish clear communication channels and collaborative frameworks that include all relevant stakeholders in emergency response planning and execution.
- Capacity Building and Knowledge Sharing: One of the significant achievements of FIRE-RES is its emphasis on capacity building and knowledge sharing. By raising awareness and promoting education on wildfire risk prevention, preparedness, and response, the project enhances the overall capacity of involved stakeholders. Applying this to command and control systems, ongoing training programs, workshops, and the development of best practices are crucial for building a common understanding and operational proficiency among different national and regional command centers.
- Human Capital Development: The FIRE-RES training event in Valabre (April 2024) highlighted that, on a human capital level, nations have personnel capable of greater integration into command and control structures but lack the experience and opportunity to do so. For command and control interoperability, it is vital to develop the skills and

experiences necessary for personnel to integrate seamlessly into broader, multi-national command frameworks. This includes creating opportunities for joint exercises and shared experiences that build trust and operational coherence.

These insights from the FIRE-RES project underscore the importance of a comprehensive approach to interoperability that includes not just technical solutions, but also organizational, procedural, and community-based strategies. They provide a valuable foundation for developing a roadmap aimed at improving interoperability among EU Civil Protection organizations.

Challenges and Opportunities

Identified Challenges: The FIRE-RES project has uncovered several significant challenges to achieving interoperability among EU Civil Protection organizations. These challenges highlight the complexities and barriers that need to be addressed to enhance cross-border cooperation effectively.

- Communication Barriers: Different communication protocols and languages used by various national civil protection agencies create significant barriers to effective collaboration. These differences can lead to misunderstandings and delays in response efforts during emergencies.
- Coordination Difficulties: Variations in command structures and decision-making processes across countries pose challenges to unified operations. Each country has its own established procedures and hierarchies, which can complicate efforts to coordinate a cohesive response during transnational emergencies.
- Administrative and Procedural Incompatibilities: Diverse administrative practices and procedural norms among EU member states further hinder interoperability. These incompatibilities can result in inefficiencies and slow down the mobilization of resources and personnel across borders, hampering overall command and control integration in the host nation.

Opportunities: Despite these challenges, there are numerous opportunities to enhance interoperability, as demonstrated by the FIRE-RES project and other EU, TIEMS, and research initiatives.

- Standardizing Procedures: Developing common procedures and protocols for emergency response can significantly enhance interoperability, while still appreciating the national structures and legislation. Standardization efforts could include creating unified guidelines for communication, resource allocation, and operational coordination, similar to the EU Host Nation Support (HNS) guidelines. In fact the EU Host Nation Support guidelines provide a good example of development of format of command and control guidelines (UCP Knowledge Network).
- Improving Communication Frameworks: Establishing robust communication frameworks that support multiple languages and protocols can bridge communication gaps. This could involve adopting interoperable communication technologies and platforms that enable real-time information sharing among different agencies (FIRE RES) (FIRE RES) (Research EU).
- Enhancing Collaborative Training Programs: Joint training programs and exercises are crucial for building trust and operational familiarity among different national teams. These programs can simulate cross-border emergency scenarios, but focus on command and control interoperability, allowing agencies to practice and refine their coordination and communication strategies (Research EU) (European Research Executive Agency). For example, the practicing of personnel exchange in command and control systems and

simulations to address functional aspects of command and control interoperability.

- **Promoting Capacity Building and Partnership Brokerage:** Capacity building initiatives, such as training and educational programs, can equip stakeholders with the skills and knowledge needed for effective collaboration. Additionally, fostering partnerships between civil protection organizations with a focus on command and control, enhances overall preparedness and response capabilities.

By addressing these challenges and leveraging the opportunities identified, EU Civil Protection organizations can significantly improve their command and control interoperability at a functional level in personnel and systems. This will not only enhance their ability to respond to cross-border emergencies but also strengthen overall disaster resilience across the region, while not forcing investment in equipment, new technologies, or infrastructure.

Elements of Command and Control Interoperability

Overview: Command and Control Interoperability in the context of EU Civil Protection organizations encompasses various potential elements that enable different national systems to work together effectively during emergencies. These characteristics are well-documented globally and offer a foundation for developing interoperability frameworks tailored to the EU's unique architecture and needs.

- **Span of Control:** Effective management and coordination of resources during emergencies require a clear span of control. This principle ensures that each supervisor oversees a manageable number of subordinates, facilitating efficient decision-making and communication. Adopting a standardized span of control can streamline operations and enhance response capabilities during large-scale emergencies.
- **Unified Command:** A unified command structure is essential for coordinated decision-making during emergencies. This structure allows multiple agencies to operate under a single, cohesive command, ensuring that all efforts are aligned, and resources are utilized efficiently. Unified command helps eliminate confusion and duplication of efforts, which is particularly important in cross-border emergency scenarios.
- **Joint Training and Exercises:** Regular, collaborative training programs and exercises are crucial for building trust and operational familiarity among different national teams. These activities allow agencies to practice and refine their coordination and communication strategies in simulated emergency scenarios. Joint training helps identify and address potential interoperability issues before they arise in real-world situations.
- **Common Terminology and Procedures:** Standardized language and procedures ensure clarity and consistency in communication and operations. By adopting common terminology and standardized procedures, EU Civil Protection agencies can reduce misunderstandings and enhance their ability to work together seamlessly. This element is particularly important for ensuring that all agencies understand each other's roles, responsibilities, and actions during emergencies.
- **Resource Sharing and Mutual Aid:** Agreements and mechanisms for sharing resources across borders are vital for effective emergency response. These arrangements allow countries to provide and receive assistance quickly, ensuring that critical resources are available where and when they are needed. Resource sharing and mutual aid agreements enhance the collective capacity of EU Civil Protection organizations to manage large-scale emergencies.

Best Practice Example:

- **Joint Drills and Integrated Response Scenarios:** The FIRE-RES project has highlighted the importance of joint drills and integrated response scenarios. These activities allow agencies to test and improve their interoperability in realistic settings, identifying strengths and areas for improvement. In terms of command-and-control interoperability, this would be an ideal point to integrate personnel in functional areas in order to create interoperability at the individual level within a command and control structure. Exemplified by the training event in Valabre, France where integrated response scenarios integrated personal from different civil protection structures. The training event provided a platform for the exchange of personnel between civil protection system, fostering realistic learning and collaboration against the backdrop of an integrated response scenario.

Tailoring to the EU Architecture: It is important to note that while these elements and best practices are globally recognized, it is crucial to define and adapt them to fit the specific needs and architecture of the EU. The diversity of administrative structures, legal frameworks, and operational procedures across EU member states necessitates a tailored approach to interoperability. Developing a detailed roadmap and project focused on these tailored solutions will ensure that interoperability efforts are practical, effective, and sustainable within the EU context.

By understanding and implementing these potential elements, and customizing them to the EU's unique context, EU Civil Protection organizations can significantly enhance their interoperability, ensuring a more coordinated and effective response to emergencies across national borders.

Potential Framework for Harmonization and Interoperability

Strategic Approach: To enhance command and control interoperability across EU Civil Protection systems, a strategic and collaborative approach is essential. Drawing lessons from existing initiatives like the EU Host Nation Support (HNS) guidelines, there is significant potential to develop a framework that aligns the diverse structures and processes of EU member states, enhancing cooperation and coordination.

Role of Interoperability: Interoperability is crucial for effective disaster response, enabling different national systems to work together seamlessly. It enhances the capacity to respond to cross-border emergencies, reduces redundancy, and maximizes resource use. A coordinated response ensures timely and efficient actions, ultimately saving lives and minimizing damage. Interoperability is being addressed through various initiatives, such as FIRE-RES, however command and control interoperability remains extant.

Pathways for Developing a Framework: Several pathways can be considered for developing a potential framework for interoperability:

- **Command and Control Guidelines (Best Practices):** Mirroring the EU HNS Guidelines effort, there is a need to develop and adopt a set of "best practices" or guidelines for command and control during response that all EU member states can follow. This includes understanding functional areas, aspects of incident management, resource allocation processes, and operational coordination mechanisms. Such standardization would facilitate smoother cooperation during cross-border emergencies, and specifically drive interoperability at depth to the personnel level.

- **Interoperable Communication Systems**: Establishing interoperable communication systems is vital for real-time information sharing among different agencies. This could involve adopting compatible technologies and platforms that support multiple languages and communication protocols, ensuring that all parties remain informed and coordinated during an emergency.

- **Joint Training and Exercises:** Implementing joint training programs and exercises that involve multiple national teams is crucial. These activities help build trust, operational familiarity, and a better understanding of each other's capabilities and procedures. Regular exercises will also identify potential interoperability issues and allow for the development of solutions in a controlled environment.

- **Legislative and Policy Alignment:** Where applicable, harmonizing laws and policies related to civil protection and emergency management across the EU will provide a consistent legal framework that supports standardized procedures and facilitates cross-border cooperation. Legislative alignment ensures that all member states have compatible policies for resource sharing, mutual aid, and operational coordination.

Example: The development of the EU HNS guidelines serves as an exemplary model for the potential to create a framework for interoperability. Just as the HNS guidelines standardized procedures for receiving and providing assistance during disasters, a similar framework could outline standardized procedures and policies to enhance coordination and cooperation in civil protection efforts.

By pursuing these pathways and aligning them with the specific needs and contexts of EU member states, there is substantial potential to develop a framework that enables more effective and coordinated disaster response efforts. This strategic approach will ensure that EU Civil Protection organizations can work together seamlessly, enhancing resilience and reducing the impact of emergencies across the region.

What's Next? Develop a Conceptual Way Ahead (Initial Roadmap)

To begin the conversation about developing command and control operability, an initial roadmap can be developed that can frame the problem and way ahead. However, a full comprehensive roadmap is required to understand the full complexity of the interoperability issue. A full and comprehensive roadmap requires funding and personnel to develop properly, and EU endorsement to provide the appropriate authority. A comprehensive roadmap will serve as a strategic guide, outlining the necessary steps, milestones, and resources required to create a framework that fosters coordination, communication, and collaboration across national borders.

Developing a detailed roadmap is essential for several reasons. First, a roadmap clarifies the role of command and control interoperability, creating a unified strategy that addresses common challenges and goals. By developing a roadmap towards command and control interoperability, there are opportunities to reduce redundancy and identify commonality amongst other EU projects. Second, a roadmap maximizes the use of available resources by identifying and prioritizing critical areas for development. This helps to ensure that funds and efforts are directed towards the most impactful initiatives, enhancing the overall effectiveness of a project to develop command and control interoperability.

A full roadmap also establishes clear milestones and performance indicators to track progress and ensure accountability throughout the implementation process. Clear milestones provide a timeline for achieving specific goals, making it easier to measure success and make adjustments as needed. Additionally, engaging all relevant stakeholders in the

development and implementation process ensures broad support and participation. By involving stakeholders from the beginning, the roadmap can reflect a wide range of perspectives and expertise, enhancing its relevance and effectiveness.

A comprehensive roadmap would include several critical components. It would begin with a comprehensive assessment of current interoperability capabilities, aligning with international standards and best practices. This initial phase would involve engaging stakeholders through consultations and workshops to gather input and ensure alignment with national priorities. By understanding the current state and desired outcomes, the roadmap can be tailored to address specific needs and challenges to achieve command and control interoperability.

By committing to the development and implementation of this roadmap, EU Civil Protection organizations can ensure they are better equipped to respond to emergencies in a coordinated and effective manner. This strategic approach will lead to the creation of a robust and resilient civil protection framework that can effectively address the complexities of modern disaster response. The roadmap will provide a shared vision and actionable plan, fostering collaboration and enhancing the collective capacity to manage cross-border emergencies.

After the Roadmap

The next phase would involve developing non-binding guidelines that outline standardized procedures and protocols for interoperability. These guidelines would be customized to address the specific needs and contexts of EU member states, ensuring relevance and applicability. Additionally, training programs would be developed to support the implementation of these guidelines, providing civil protection agencies with the knowledge and skills needed to effectively collaborate across borders and effectively integrate into other command and control structures.

The development of the EU Host Nation Support (HNS) guidelines serves as an exemplary model for creating a framework for interoperability. Just as the HNS guidelines standardized procedures for receiving and providing assistance during disasters, an interoperability roadmap would outline standardized procedures and policies to enhance coordination and cooperation in civil protection efforts.

Pilot projects would be implemented to test the proposed solutions and frameworks in real-world scenarios. These pilot projects would provide valuable insights into the effectiveness of the guidelines and training programs, allowing for data collection and feedback to refine and improve the approach. By evaluating the success of these pilots, adjustments can be made to ensure the framework is robust and effective.

Following the pilot phase, the interoperability framework would be rolled out across all EU member states. This full-scale implementation would involve providing ongoing support and resources to facilitate adoption and ensure success. A feedback mechanism would be established to gather input from the field, allowing for continuous improvement of the framework based on real-world experiences.

Ensuring the long-term commitment to interoperability would require securing funding and resources to support ongoing efforts. Integrating the interoperability framework with other relevant EU initiatives and international organizations would ensure alignment and synergy, enhancing the overall impact of the efforts.

Conclusion

Interoperability among EU Civil Protection organizations is not just a desirable goal but an essential requirement for effective disaster response and resilience. As cross-border emergencies become increasingly frequent and complex, the ability of different national systems to work together seamlessly is crucial. The insights from TIEMS and findings from the FIRE-RES project highlight significant challenges and opportunities in achieving command and control interoperability, emphasizing the need for a coordinated and strategic approach.

The proposed development of a comprehensive roadmap represents a vital step towards enhancing interoperability. This roadmap will serve as a strategic guide, outlining the necessary steps, milestones, and resources required to foster coordination, communication, and collaboration across national borders. By aligning strategies, maximizing resources, establishing clear milestones, and engaging stakeholders, the roadmap will provide a structured and effective approach to achieving interoperability.

Key components of the roadmap will include a comprehensive assessment of current capabilities, the development of non-binding guidelines and customized training programs, the implementation and evaluation of pilot projects, and the full-scale rollout of the interoperability framework. Ensuring long-term commitment and integrating the framework with other relevant initiatives will be crucial for sustained success.

The development of the EU Host Nation Support (HNS) guidelines serves as an exemplary model for creating a framework for interoperability. Just as the HNS guidelines standardized procedures for receiving and providing assistance during disasters, a command and control interoperability roadmap would outline standardized procedures and policies to enhance coordination and cooperation in civil protection effort.

By committing to the development and implementation of this roadmap, EU Civil Protection organizations can significantly enhance their ability to respond to emergencies in a coordinated and effective manner. This strategic approach will lead to the creation of a robust and resilient civil protection framework that can effectively address the complexities of modern disaster response. The roadmap will provide a shared vision and actionable plan, fostering collaboration and enhancing the collective capacity to manage cross-border emergencies.

In conclusion, the journey towards command and control interoperability requires a collective effort, informed by research, guided by strategic planning, and sustained by continuous improvement. By initiating this discussion and committing to the development of a comprehensive roadmap, we can pave the way for a more resilient and cooperative future for EU Civil Protection organizations.

Navigating cybersecurity investments in the time of NIS 2

The latest report of the European Union Agency for Cybersecurity (ENISA) aims to support policy makers in assessing the impact of the current EU cybersecurity framework, and particularly the NIS 2 Directive, on cybersecurity investments and the overall maturity of organisations in scope.

The fifth iteration of the NIS Investments report provides key insights into how organisations in scope of the NIS 2 Directive allocate their cybersecurity budgets, build their capabilities, and mature in line with the Directive's provisions, while also exploring global cybersecurity trends, workforce challenges, and the impact of AI.

The report further provides insights into the readiness of entities to comply with new requirements introduced by key horizontal (e.g. CRA) and sectorial (e.g. DORA, NCCS) legislation, while also exploring the challenges they face.

The EU Agency for Cybersecurity Executive Director, Juhan Lepassaar, highlighted: "The NIS 2 Directive signifies a turning point in Europe's approach to cybersecurity. Within a fast evolving and complex threat landscape, the proper implementation of the NIS 2 requires adequate investments and especially into the new sectors which fall under the scope of the updated Directive. The ENISA NIS Investments report provides evidence-based feedback to policymakers and stakeholders regarding NIS-driven investments. These insights are essential for informed decision-making and addressing potential hurdles and gaps in cybersecurity policy implementation."

The 2024 edition features a significant enhancement compared to previous versions, as it extends the survey sample to include sectors and entities that are in scope of NIS 2. Through this approach, this report provides a pre-implementation snapshot of relevant metrics for the new sectors and entities under NIS 2, laying a foundation for future assessments of the impact of NIS 2. Additionally, it includes a sectorial deep dive in the Digital infrastructure and Space sectors.

Data were collected from 1350 organisations from all EU Member States covering all NIS2 sectors of high criticality, as well as the manufacturing sector.

Key findings

- Information security now represents 9% of EU IT investments, a significant increase of 1.9 percentage points from 2022, marking the second consecutive year of growth in cybersecurity investment post-pandemic.

- In 2023, median IT spending for organisations rose to EUR 15 million, with information security spending doubling from EUR 0.7 million to EUR 1.4 million.

- For the fourth consecutive year, the percentage of IT Full Time Equivalents (FTEs) dedicated to information security has declined, from 11.9% to 11.1%. This decrease may reflect recruitment challenges, with 32% of organisations—and 59% of SMEs—struggling to fill cybersecurity roles, particularly those requiring technical expertise. This trend is especially notable given that 89% of organisations expect to need additional cybersecurity staff to comply with NIS2.

New NIS2 sectors are comparable in cybersecurity spending to existing NIS Directive entities, with their investments largely focused on developing and maintaining baseline cybersecurity capabilities. Emerging areas, such as post-quantum cryptography, receive limited attention with only 4% of surveyed entities investing and 14% planning future investments.

- The majority of organisations anticipate a one-off or permanent increase in their cybersecurity budgets for compliance with NIS 2. Notably, a substantial number of entities will not be able to ask for the required additional budget, a percentage that is especially high for SMEs (34%).

- 90% of entities expect an increase in cyberattacks next year, in terms of volume, costliness or both. Despite that, 74% focus their cybersecurity preparedness efforts internally, with much lower participation in national or EU-level initiatives. This gap underscores a critical area for improvement, as effective cross-border cooperation in managing large-scale incidents can only be achieved at these higher levels.

- Overall awareness among in-scope entities is encouraging, with 92% being aware of the general scope or specific provisions of the NIS 2 Directive. However, a notable percentage of entities in certain new NIS 2 sectors remain unaware of the Directive, suggesting a potential need for increased awareness campaigns by the national competent authorities.

- Entities in sectors already covered by NIS outperform those newly included under NIS 2 across various cybersecurity governance, risk, and compliance metrics. Similarly, entities in new NIS 2 sectors show lower engagement and higher non-participation rates in cybersecurity preparedness activities. This highlights the positive impact the NIS Directive has had on the sectors already in scope; and creates anticipation for the impact NIS 2 will have on the new sectors.

Through the years, the series of the NIS Investments report provide a rich historical dataset which, building on this year's foundation, will allow us to gain insights into the effect of NIS 2 on new entities within its scope.

Stop the Scams: FS-ISAC's New Phishing Prevention Framework Helps Financial Sector Counter Surge in Scams

FS-ISAC, the member-driven, not-for-profit organization that advances cybersecurity and resilience in the global financial system, today has introduced Stop the Scams: A Phishing Prevention Framework for Financial Services. This comprehensive framework aims to help financial services firms counter a surge in phishing attacks, the most reported type of cybercrime worldwide. With phishing scams increasingly impacting both firms and consumers, Stop the Scams offers critical, actionable steps to help firms safeguard themselves and their customers against the financial and reputational harm caused by phishing.

Phishing scams typically involve fraudsters using email, text messages, or phone calls that mimic trusted sources, such as banks or financial firms, to steal personal and financial information. Victims of these scams may face significant financial loss, while their financial service providers may bear responsibility for reimbursing or supporting them. Recognizing the need for a cohesive solution designed to help financial firms of all sizes and maturity levels reduce phishing reports, FS-ISAC's Fraud Strategy Working Group collaborated with leading member firms to develop Stop the Scams.

The Framework has already delivered impressive results, with three major US banks reporting a reduction in text abuse incidents by over 50% shortly after implementation. The core approach consists of four essential actions:

- Collect and Share Intelligence: Gather actionable intelligence from consumers and disseminate it across relevant departments.

- Educate Employees and Customers: Develop education programs to heighten awareness of phishing tactics among both employees and customers.

- Catalog Communication Channels: Maintain a catalog of telephone numbers used by the institution and third-party partners to prevent spoofing.

- Leverage Anti-Phishing Technology: Collaborate with telecommunications providers to deploy anti-phishing solutions.

Linda Betz, Executive Vice President of Global Community Engagement at FS-ISAC, emphasized the significance of collective action, stating, "Phishing has become a global epidemic affecting millions, yet by working together, financial firms can develop highly effective defenses. Our Stop the Scams framework provides a strategic roadmap, supporting firms in fighting phishing through shared knowledge and coordinated intelligence that can shift the balance against cybercriminals."

To further maximize the Framework's effectiveness, FS-ISAC recommends two best practices:

- Establish a Structured Reporting Intake Process: Design a fraud and phishing intake process with clear, concise questions to gather actionable intelligence while minimizing the burden on consumers.

- Build an Abuse Inbox for Reporting: Set up an "abuse box" infrastructure, enabling consumers to report phishing attempts. This approach allows financial services firms to gather timely threat insights, benefiting both internal teams and the broader financial sector.

"The actions in the Stop the Scams framework provide concrete steps for helping to reduce phishing incidents and strengthen protections amid the fast-changing threat landscape and rapidly evolving technologies such as generative AI," said Susan Koski, Chief Information Security Officer at PNC. "We hope that this comprehensive framework will advance the industry's battle against these attacks."

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

CLOSING COMMENTS - CRITICAL INFRASTRUCTURE PROTECTION & RESILIENCE EUROPE (CIPRE) & CIP WEEK

12th-14th November 2024, Madrid, Spain

Critical Infrastructure Protection Week in Europe
12th-14th November 2024 - Madrid, Spain
International Association of CIP Professionals
PARTNER EVENTS:
critical infrastructure PROTECTION AND RESILIENCE EUROPE
EU-CIP

Before we all head off home, or go to the bar for a light refreshment, if there was a bar in this hotel! I just wanted to say a few words in closing the conference and Critical Infrastructure Protection (CIP) Week.

It has been fantastic to be here in Madrid with so many talented, professional and charming people. The networking and learning opportunities at events such as these are priceless so I do hope that you have found the last few days to have been educational, enjoyable and of real value.

The conference had great opening keynote and plenary sessions, followed by two days of hot topics, discussions and workshops as well as an exhibition with leading technologies and solutions for protection of critical infrastructures from both cyber and physical threats.

We have had some excellent presentations from some very distinguished and experienced people and some great debates around a whole range of infrastructure and information issues.

We are extremely grateful for the support we have received from The National Center for the Protection of Critical Infrastructures here in Spain and to all our speakers, sponsors and exhibitors without whose continuing support events such as these would not be possible.

We were delighted to launch CIP week in partnership with our colleagues from the EU-CIP Horizon Project. The combination of CIPRE and EU-CIP is the first of its kind to seek to develop and inform thinking around the current challenges and the impact of the new EU Directives alongside the developing complexities of the threat environment against European critical entities.

We had a great start on Tuesday with the Keynote session. Jose Luis Perez Pajuelo, the Director General of the National Center for the Protection of Critical Infrastructures within the Spanish Ministry of Interior started the conference. He provided some clear messaging around their Governments strategic focus on developing resilience and the need for continued efforts in pursuit of the unravelling the complexities of collective activity through enhanced levels of cooperation and coordination between the Public and Private sectors (PPPs).

Jose was a strong advocate of moving towards embracing a ‘whole society’ approach to protection and resilience involving

multiple stakeholders and importantly providing a greater role for the inclusion of communities. The theme of the need for enhanced levels of cooperation and cooperation continued throughout the keynote session and beyond culminating with a whole session dedicated to collaboration. Information sharing and enhancing PPPs taking place on the final day of the conference.

The second keynote speaker was Juan Diez Gonzalez, the Head of Cybersecurity for strategic Healthcare, Food and Research sectors within the Spanish National Cybersecurity Institute (INCIBE). Juan updated conference delegates on the developing activities designed to boost cyber security in line with the Spanish National Security Strategy stating that the 'rules of the game' are changing within the country.

The next keynote speaker was Catherine Piana, the Secretary General of the Confederation of European Security Services (CoESS). Catherine shared her views on the evolving state of critical infrastructure protection in Europe. She emphasized the importance of seeing security as the enabler that it is, and not a cost, a necessary evil or an obstacle to trade.

She highlighted the need for public-private partnerships, cross-border cooperation, and a whole-of-society approach to security adding that by cultivating a strong security culture and encouraging information sharing, we can address complex, interconnected threats and protect Europe's essential services. Her closing words, delivered with a big smile on her face, spoke of the need to be aware of the fact that security personnel can be just a little paranoid with big imaginations seeing that everything that can go wrong will go wrong.

The final presentation of the session was delivered by Email Gugliandolo who is currently the EU-CIP Project Coordinator. She provided a level of detail on the EU-CIP project which was launched in October 2022 and designed to finish in September 2025. It being an EU funded project under Horizon Europe bringing together 20 partners seeking to establish a novel pan European knowledge network for resilient Infrastructures. Emilia also outlined the agenda and aims of their second annual conference taking place on the 2nd day of CIP week.

Resilience obviously remained as a major theme and we had several references to the fact that the month of November in the United States is usually recognised as 'Critical Infrastructure Security and Resilience Month (CISR)'. This highlights the importance of reminding asset owners and operators to step up and focus on safeguarding vital critical installations. The Cybersecurity and Infrastructure Security Agency (CISA) leads on this national effort under their enduring theme of 'Resolve to be Resilient'.

The first plenary session covered the implementation and impacts of the Critical Entities Resilience (CER) and Network and Information Systems 2 (NIS2) Directives. This was an extremely informative session with a broad range of presenters highlighting the current position and the emerging issues from a number of differing perspectives.

The tried and tested Twin Track format kicked off both days two and three covering a whole range of topics. Natural Disasters and their impact on both infrastructure and information was obviously topical however, I was surprised that we did not hear more on the subject so soon and being in such close proximity to the dreadful flooding in Valencia.

Cyber was a significant theme over all three days and we heard

WELCOME
OTORIO

KnowBe4
Strengthen Your Security Culture and Reduce Human Risk

what some of the top cyber-attacks in 2024 were, including, Ransomware, Phishing and Denial of Service being just a few within the top ten. We had reminders from several speakers of the need to continually develop our defences with Luanda Domi from the Global Forum on Cyber Expertise (GFCE) eloquently stating that we need to collectively, Connect-Strengthen and Advance our cyber efforts to meet both the current and future challenges.

The array of topics covered were wide-ranging and included, Emerging Threats right through to Crisis and Risk Management. We touched on terrorism but not in any real depth and explored a great deal on the technologies available to detect and protect, some of which were on display with our exhibitors. Other issues of note that were of particular interest were around the growth of concern with Insider Threats and the need for continued efforts to enhance Public Private Partnerships.

The final session on Thursday afternoon was an interactive workshop designed on the theme of: ‘What If: Exploring Critical Infrastructure Cascading Effects’. The was ably delivered by Alessandro Lazari and Dr Monica Cardarilli. They posed a number of challenging situations to the delegates, creating significant levels of discussion and a variance of views from across the audience.

It was interesting to note that throughout the 3 days there were over 1000 slides presented, some had very pretty pictures, some were extremely informative, some were very busy with hundreds of words on the one slide and then we had a couple which depicted mathematical equations on probability, which did take some explaining!

I loved all the slides but in terms of relevance I particularly liked the one providing a quote from Albert Einstein, ‘We cannot solve our problems with the same thinking we used when we created them’.

Overall though the quality of speakers and presentations were tremendous, the facilities were excellent and we will all go away having learned hundreds of new acronyms. It does seem that not much can be done across infrastructure and information sectors unless it has a good solid acronym in place. In fact, one of the speakers did state that you will not get any of the billions of Euros of Horizon funding for any new programme of activity unless you have at least 20 or so new acronyms within your proposal. The best one of the week for me was – SSSCIP which represents the Ukrainian ‘State Service of Special Communication and Information Protection’ - just brilliant.

In closing, finally, I do hope that you have all had a great time here in Madrid and that you go away:

- Having learned something new
- Having made new professional contacts, who may be able to assist you in some way and importantly -
- Having made new friends.

Once again, I just want to thank our supporters, our speakers, our sponsors and exhibitors and most of all, thank you for your attendance and active participation.

John Donlon QPM FSyL
Conference Chairman
Chairman, IACIPP

Mobile and Banking Industries Join Forces to Fight Fraud

GSMA and UK Finance have joined forces to provide a collaborative framework for the UK's leading mobile network operators and banks to develop and launch Scam Signal, a new solution to help address Authorised Push Payment (APP) fraud in the UK. Scam Signal is launching as a collaboration between mobile network operators EE, Virgin Media O2, Three, Vodafone and UK Finance members, including NatWest, participating on behalf of the banking industry.

The new solution, which is delivered via an Application Programmable Interface (API), enables banks to better identify and stop fraudulent bank transfers by analysing real-time network data and identifying correlations between phone calls and fraudulent bank transfers.

Data from UK Finance shows that £213.7 million was lost to APP fraud in the first half of 2024. This is where criminals manipulate customers into transferring money to a criminal. In terms of the value of losses, 35 per cent of APP losses originated from scams which started through telecommunication. This is where criminals contact victims through SMS and telephone often purporting to be from legitimate organisations, such as a bank.

To help protect UK banking customers, GSMA and UK Finance began discussions between their members to understand how the high volumes of real-time mobile network data could help UK banking identify suspicious calls and other activities. Through a series of workshops with MNO and bank representatives, and the modelling and analysis of network data, correlations with fraudulent bank transfers were identified which formed the basis of the Scam Signal solution.

Early development of Scam Signal was spearheaded by Vodafone, with the mobile operator completing a successful three-month pilot project which resulted in scam detection improving by 30 per cent at a major UK bank.

Dianne Doodnath, Principal of Economic Crime at UK Finance, said: "Fraud remains a major problem, with our data showing that over £210 million was stolen by criminals through APP fraud in the first half of 2024. APP fraud originating from telephone calls or SMS continues to be of higher value and accounted for 35 per cent of losses.

"To address social engineering tactics used by criminals, cross-industry collaboration has once again proven critical. Working with GSMA has been invaluable in making UK mobile network operators available to support and analyse data with our financial services members. This collaboration has resulted in a strong solution that should have a real impact by identifying criminal activity and increasing fraud detection."

Brian Gorman, Fintech Lead at GSMA, said: "It is great to see the result of our members' collaboration directly addressing that problem and providing significant benefit to the UK public – Scam Signal is already detecting fraudulent calls and stopping transactions to criminals. Delivering this solution was made possible by the close collaboration between our members and UK Finance and its members; and we are looking forward to continuing our valuable work together."

As demonstrated by the success to-date of the GSMA's Open Gateway initiative, the API economy is critical to unlocking mobile network capabilities and leveraging industry insights to support a growing range of services, including anti-fraud and identification APIs. Spanning the globe from Brazil to China, Germany to South Africa, we are seeing the mobile industry come together to launch universal network APIs such as SIM Swap and Number Verify to combat online fraud and protect customers.

World Border Security Congress

25th-27th March 2025

Madrid, Spain

www.world-border-congress.com

Co-hosted and Supported by: GOBIERNO DE ESPAÑA · MINISTERIO DEL INTERIOR · GUARDIA CIVIL

Patrolling the Periphery - Developing Border Strategies Through Co-operation and Technology

REGISTRATION OPEN

Register today and save with Early Bird Delegate Rates

Spain's vast coastline and strategic location between Africa and Europe present unique challenges for the National Police and Guardia Civil.

Spain faces a constant influx of migrants seeking a better life in Europe. The Canary Islands and the enclaves of Ceuta and Melilla, bordering Morocco, are popular entry points. Patrolling these vast stretches, especially maritime borders, requires significant resources.

Spain is also a key entry point for hashish from Morocco and cocaine from South America destined for other European countries. The decentralized nature of trafficking groups makes it difficult to infiltrate and dismantle them.

The country, and region's, border security landscape is constantly evolving. By addressing these challenges through international collaboration, innovative technologies, and strategic resource allocation, the international border security community can strive towards a more secure future.

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 Madrid, Spain on 25th-27th March 2025 for the next gathering of international border security, protection and migration management professionals.

www.world-border-congress.com

Confirmed Speakers include:

- Hans Leijtens, Executive Director, FRONTEX
- James Collins, Assistant Commissioner, U.S. Customs and Border Protection (CBP)
- Samir Krasniqi, Coordinator of the National Center for Border Management (NCBM), Ministry of Internal Affairs, Republic of Kosovo
- Vice Admiral Robert Patrimonio, Commander, Maritime Security Law Enforcement Command, Philippines Coast Guard
- Amanda Read, National Vulnerability Lead, UK Border Force
- Enkhtur Adiyajav, Head of PIU, Passenger Information Unit, Mongolia
- Ibrahim Imam Haafiz, National Imam/ Dept Head Religious Affairs Unit, Ghana Immigration Service
- Dr Vesna Tasevska-Dudeska, Chief Inspector for Foreigners and Readmission, Ministry of Interior, Republic of North Macedonia
- George-Okoli Francisco Chidi, Director of Programs, West African Action Network on Small Arms (WAANSA) Nigeria

View full speaker line up at www.world-border-congress.com

for the international border management and security industry

Supported by:

European Association of Airport and Seaport Police · AFRICAN UNION · ISIO · International Association of CIP Professionals · NSaRC

Media Partners:

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

Groundbreaking Framework for the Safe and Secure Deployment of AI in Critical Infrastructure Unveiled by Department of Homeland Security

The Department of Homeland Security (DHS) has released a set of recommendations for the safe and secure development and deployment of Artificial Intelligence (AI) in critical infrastructure, the "Roles and Responsibilities Framework for Artificial Intelligence in Critical Infrastructure" ("Framework"). This first-of-its kind resource was developed by and for entities at each layer of the AI supply chain: cloud and compute providers, AI developers, and critical infrastructure owners and operators – as well as the civil society and public sector entities that protect and advocate for consumers. The Artificial Intelligence Safety and Security Board ("Board"), a public-private advisory committee established by DHS Secretary Alejandro N. Mayorkas, identified the need for clear guidance on how each layer of the AI supply chain can do their part to ensure that AI is deployed safely and securely in U.S. critical infrastructure. This product is the culmination of considerable dialogue and debate among the Board, composed of AI leaders representing industry, academia, civil society, and the public sector. The report complements other work carried out by the

Administration on AI safety, such as the guidance from the AI Safety Institute, on managing a wide range of misuse and accident risks.

America's critical infrastructure – the systems that power our homes and businesses, deliver clean water, allow us to travel safely, facilitate the digital networks that connect us, and much more – is vital to domestic and global safety and stability. These sectors are increasingly deploying AI to improve the services they provide, build resilience, and counter threats. AI is, for example, helping to quickly detect earthquakes and predict aftershocks, prevent blackouts and other electric-service interruptions, and sort and distribute mail to American households. These uses do not come without risk, and vulnerabilities introduced by the implementation of this technology may expose critical systems to failures or manipulation by nefarious actors. Given the increasingly interconnected nature of these systems, their disruption can have devastating consequences for homeland security.

"AI offers a once-in-a-generation opportunity to improve the strength and resilience of U.S. critical infrastructure, and we must seize it while minimizing its potential harms. The Framework, if widely adopted, will go a long way to better ensure the safety and security of critical services that deliver clean water, consistent power, internet access, and more," said Secretary Alejandro N. Mayorkas. "The choices organizations and individuals involved in creating AI make today will determine the impact this technology will have in our critical infrastructure tomorrow. I am grateful for the diverse expertise of the Artificial Intelligence Safety and Security Board and its members, each of whom informed these guidelines with their own real-world experiences developing, deploying, and promoting the responsible use of this extraordinary technology. I urge every executive, developer, and elected official to adopt and use this Framework to help build a safer future for all."

If adopted and implemented by the stakeholders involved in the development, use, and deployment of AI in U.S. critical infrastructure, this voluntary Framework will enhance the harmonization of and help operationalize safety and security practices, improve the delivery of critical services, enhance trust and transparency among entities, protect civil rights and civil liberties, and advance AI safety and security research that will further enable critical infrastructure to deploy emerging technology responsibly. Despite the growing importance of this technology to critical infrastructure, no comprehensive regulation currently exists.

DHS identified three primary categories of AI safety and security vulnerabilities in critical infrastructure: attacks using AI, attacks targeting AI systems, and design and implementation failures. To address these vulnerabilities, the Framework recommends actions directed to each of the key stakeholders supporting the development and deployment of AI in U.S. critical infrastructure as follows:

- **Cloud and compute infrastructure providers** play an important role in securing the environments used to develop and deploy AI in critical infrastructure, from vetting hardware and software suppliers to instituting strong access management and protecting the physical security of data centers powering AI systems. The Framework encourages them to support customers and processes further downstream of AI development by monitoring for anomalous activity and establishing clear pathways to report suspicious and harmful activities.
- **AI developers** develop, train, and/or enable critical

infrastructure to access AI models, often through software tools or specific applications. The Framework recommends that AI developers adopt a Secure by Design approach, evaluate dangerous capabilities of AI models, and ensure model alignment with human-centric values. The Framework further encourages AI developers to implement strong privacy practices; conduct evaluations that test for possible biases, failure modes, and vulnerabilities; and support independent assessments for models that present heightened risks to critical infrastructure systems and their consumers.

- **Critical infrastructure owners and operators** manage the secure operations and maintenance of key systems, which increasingly rely on AI to reduce costs, improve reliability and boost efficiency. They are looking to procure, configure, and deploy AI in a manner that protects the safety and security of their systems. The Framework recommends a number of practices focused on the deployment-level of AI systems, to include maintaining strong cybersecurity practices that account for AI-related risks, protecting customer data when fine-tuning AI products, and providing meaningful transparency regarding their use of AI to provide goods, services, or benefits to the public. The Framework encourages critical infrastructure entities to play an active role in monitoring the performance of these AI systems and share results with AI developers and researchers to help them better understand the relationship between model behavior and real-world outcomes.

- **Civil society**, including universities, research institutions, and consumer advocates engaged on issues of AI safety and security, are critical to measuring and improving the impact of AI on individuals and communities. The Framework encourages civil society's continued engagement on standards development alongside government and industry, as well as research on AI evaluations that considers critical infrastructure use cases. The Framework envisions an active role for civil society in informing the values and safeguards that will shape AI system development and deployment in essential services.

- **Public sector entities**, including federal, state, local, tribal, and territorial governments, are essential to the responsible adoption of AI in critical infrastructure, from supporting the use of this technology to improve public services to advancing standards of practice for AI safety and security through statutory and regulatory action. The United States is a world leader in AI; accordingly, the Framework encourages continued cooperation between the federal government and international partners to protect all global citizens, as well as collaboration across all levels of government to fund and support efforts to advance foundational research on AI safety and security.

President Biden directed Secretary Mayorkas to establish the Board to advise the Secretary, the critical infrastructure community, other private sector stakeholders, and the broader public on the safe and secure development and deployment of AI technology in our nation's critical infrastructure. Secretary Mayorkas convened the Board for the first time in May 2024, and Board Members identified a number of issues impacting the safe use and deployment of this technology, including: the lack of common approaches for the deployment of AI, physical security flaws, and a reluctance to share information within industries.

The Framework is designed to help address these concerns and complements and advances existing guidance and analysis from the White House, the AI Safety Institute, the Cybersecurity and Infrastructure Security Agency, and other federal partners.

"Ensuring the safe, secure, and trustworthy development and use of AI is vital to the future of American innovation and critical to our national security. This new Framework will complement the work we're doing at the Department of Commerce to help ensure AI is responsibly deployed across our critical infrastructure to help protect our fellow Americans and secure the future of the American economy." – Secretary of Commerce, Gina Raimondo

"The Framework correctly identifies that AI systems may present both opportunities and challenges for critical infrastructure. Its developer-focused provisions highlight the importance of evaluating model capabilities, performing security testing, and building secure internal systems. These are key areas for continued analysis and discussion as our understanding of AI capabilities and their implications for critical infrastructure continues to evolve." *– Dario Amodei, CEO and Co-Founder, Anthropic*

"I would like to thank the Board for their leadership in developing this important Framework and appreciate the opportunity to provide input that reflects critical infrastructure needs. AI holds the promise to create significant opportunities for our world, but we must ensure the technology is deployed thoughtfully and responsibly. The Framework, developed through countless hours of collaboration and negotiation, provides a foundation for how business, government, and all segments of our society can work together to enhance accountability, integration, and cooperation. I'm looking forward to continued work with our partners in this effort." – *Ed Bastian, CEO, Delta Air Lines*

"The AI Roles and Responsibilities Framework promotes collaboration among all key stakeholders with a goal of establishing clear guidelines that prioritize trust, transparency and accountability — all essential elements in harnessing AI's enormous potential for innovation while safeguarding critical services. Salesforce is committed to humans and AI working together to advance critical infrastructure industries in the U.S. We support this framework as a vital step toward shaping the future of AI in a safe and sustainable manner." *– Marc Benioff, Chair and CEO, Salesforce*

"Humane Intelligence fully endorses the 'Roles and Responsibilities Framework for Artificial Intelligence in Critical Infrastructure,' developed by the AI Safety and Security Board. This comprehensive framework offers essential guidance for the responsible and secure use of AI across the United States. As an organization dedicated to advancing safe and ethical AI practices, we believe the voluntary responsibilities outlined are crucial steps toward enhancing the safety, security, and trustworthiness of AI systems. By addressing five key roles – cloud and compute infrastructure providers, AI developers, critical infrastructure owners and operators, civil society, and the public sector – the Framework thoughtfully recognizes the diverse stakeholders involved in safeguarding our nation's critical infrastructure. The emphasis on securing environments, driving responsible model and system design, implementing data governance, ensuring safe and secure deployment, and monitoring performance and impact aligns closely with our mission. We commend the AI Safety and Security Board for providing clear technical and process recommendations that will help ensure AI systems not only function effectively but also serve the public good in a safe and ethical manner. Humane Intelligence is committed to

supporting these principles and will continue working with partners across sectors to promote the responsible development and deployment of AI in critical infrastructure." – *Dr. Rumman Chowdhury, CEO & Co-founder, Humane Intelligence*

"This Framework recognizes that proper governance of AI in the critical infrastructure ecosystem is a multistakeholder endeavor. If companies, governments, and NGOs embrace the voluntary roles and responsibilities this Framework envisions, deployment of AI in critical infrastructure is more likely to protect security, privacy, civil rights, and civil liberties than would otherwise be the case." – *Alexandra Reeve Givens, President and CEO, Center for Democracy & Technology*

"Artificial intelligence has incredible potential to create efficiencies and innovations, and this Framework takes a thoughtful approach to balancing those opportunities with the risks and challenges it creates. Partnership and collaboration between the public and private sectors will be critical as we work to incorporate these advances into infrastructure and services while also taking steps to mitigate potential harm. This Framework represents an important step towards fostering accountability, safety, and security while embracing this technology and the future." – *Bruce Harrell, Mayor of Seattle*

"We are pleased that the Roles and Responsibilities Framework prioritizes civil rights to ensure the equitable deployment of AI. The Framework reflects an understanding that in order for our nation's critical infrastructure to be best protected, AI must first be safe and effective. That starts with ensuring that all applications of AI both defend and promote equal opportunity. The DHS Framework makes significant progress toward meeting those goals." – *Damon Hewitt, President and Executive Director, Lawyers' Committee for Civil Rights Under Law*

"We are proud to be part of the U.S. Department of Homeland Security's AI Safety and Security Board to develop a Framework that will help encourage the responsible use of AI in the energy industry while ensuring critical infrastructure is protected from cyber threats. With our companywide focus on safety, resilience, and driving innovation, we plan to adopt the Framework in the relevant aspects of our business to promote the further integration of advanced AI technologies in support of sustainable energy development." – *Vicki Hollub, President and CEO, Occidental Petroleum*

"As we move into the AI era, our foremost responsibility is ensuring these technologies are safe and beneficial. The DHS AI Framework provides guiding principles that will help us safeguard society, and we support this effort." – *Jensen Huang, Founder and CEO, NVIDIA*

"The DHS Roles and Responsibilities Framework for Artificial Intelligence in Critical Infrastructure is a powerful tool to help guide the responsible deployment of AI across America's critical infrastructure and IBM is proud to support its development. We look forward to continuing to work with the Department to promote shared and individual responsibilities in the advancement of trusted AI systems." – *Arvind Krishna, Chairman and CEO, IBM*

"Academia and civil society are vital to deploying AI in critical infrastructure safely. This is a crucial, nonpartisan issue with profound impacts on the nation's well-being. This Framework reaffirms the commitment to security, transparency, and public trust. Through rigorous research and cross-sector collaboration, we can help create a resilient AI ecosystem that prioritizes the public good." – *Fei-Fei Li, Ph.D., Co-Director, Stanford Human-centered Artificial Intelligence Institute*

"Artificial Intelligence technology is already here. The only question is whether we choose to be proactive or reactive when it comes to leveraging the benefits of AI and guarding against vulnerabilities. I applaud the Biden-Harris Administration and the work of the U.S. Department of Homeland Security's AI Safety and Security Board for their commitment to seizing this moment and putting forth a responsible Framework that will benefit the American people. In partnership, Maryland will continue to work with federal leaders to unlock the power of innovation so we can deliver real results for our communities." – *Wes Moore, Governor of Maryland*

"Technology must be built on a foundation of integrity at the highest levels, and DHS's Roles and Responsibilities Framework for Artificial Intelligence in Critical Infrastructure will ensure the public and private sectors work closely together to enable AI solutions that are secure, reliable, and trustworthy. As a leader in networking and security that will connect and protect the responsible AI revolution, Cisco is proud to have contributed to the Framework alongside important government, industry, and civil society partners. We look forward to supporting the efforts by Secretary Mayorkas and the Department of Homeland Security." – *Chuck Robbins, Chair and CEO, Cisco; Chair, Business Roundtable*

"The collaboration between government, industry, and civil society organizations proved beneficial in establishing the DHS 'Roles and Responsibilities Framework for AI in Critical Infrastructure' to protect the nation's assets. The Framework lays out principles for safe and secure AI that averts anticipated and unforeseen risks, and places equal importance on the preservation of civil and human rights for the people and communities impacted by emerging technologies. The Board's intention to harmonize these goals is a promising first step in the future application and adherence to the Framework." – *Nicol Turner Lee, Ph.D., Senior Fellow and Director of the Center for Technology Innovation, Brookings Institution*

"The use of AI in critical infrastructure merits strong measures to prevent harm and ensure everyone has equal access to information, goods, and services. DHS's outlining of stakeholders' roles and responsibilities is an important first step to protecting everyone in the U.S. from discrimination in the deployment of AI systems in our nation's infrastructure." – *Maya Wiley, President and CEO, The Leadership Conference on Civil and Human Rights*

DHS is responsible for the overall security and resilience of the nation's critical infrastructure, which hundreds of millions of Americans rely on every day to light their homes, conduct business, exchange information, and put food on the table. In the 2025 Homeland Threat Assessment, the Department advised that domestic and foreign adversaries will continue to threaten the integrity of our nation's critical infrastructure due to the cascading impacts on U.S. industries and our standard of living. These threats range from, but are not limited to, the use of AI to span or scale physical attacks; targeted attacks on AI systems supporting critical infrastructure; and failures in AI design and implementation that affect critical infrastructure operations.

Singapore and ASEAN Member States Deepen Commitment to Enhance Collective Cybersecurity in the Region

Mrs Josephine Teo, Minister for Digital Development and Information and Minister-in-charge of Smart Nation and Cybersecurity and representatives of the ASEAN Member States (AMS) reaffirmed their commitment to strengthen cyber resilience in the region during the 9th ASEAN Ministerial Conference on Cybersecurity (AMCC).

Since its inception, AMCC has served as an important non-formal regional platform that brings together relevant ASEAN Ministers of Telecommunications and/or Cybersecurity which has made significant progress in advancing cross-cutting and wide-ranging discussions on possible areas for ASEAN regional cybersecurity cooperation. This includes capacity building programmes under the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) in Singapore, and the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) in Thailand. The active participation from AMS and its Dialogue Partner countries at the AMCC underlines the importance of maintaining an open, safe, secure, stable, accessible, interoperable, peaceful, and resilient cyberspace and the relevance of AMCC as a forum to facilitate collaborations.

Launch of the physical facility of ASEAN Regional CERT

At AMCC, Minister Josephine Teo announced the launch of the physical facility of the ASEAN Regional Computer Emergency Response Team (CERT). Since October 2022, Singapore has worked with AMS to draft the Operational Framework that outlines the purpose, scope, composition and partners, functions, and mechanism of the ASEAN Regional CERT. The Operational Framework was successfully endorsed by AMS at the 3rd ADGMIN in February 2023. In February 2024, the AMS also agreed for Singapore to fund and host the physical facility of the ASEAN Regional CERT for up to 10 years. The operationalisation of the ASEAN Regional CERT will amount to USD 10.1 million for 10 years which will be funded by Singapore as the current ADGMIN Chair.

The ASEAN Regional CERT will be co-located at the ASCCE in Singapore and will significantly move forward information sharing among AMS on cyber threats and attacks as well as online scams. It will serve as a dedicated space for in-person activities e.g. cyber exercises, workshops and CERT-CERT cyber capacity building programmes to foster cohesive collaboration among the AMS. The ASEAN Regional CERT Taskforce, led by a rotating overall coordinator based on the AMS' ASEAN Network Security Action Council (ANSAC) chairmanship term, will guide the efforts of the ASEAN Regional CERT.

The inaugural ASEAN Regional CERT Taskforce meeting was chaired by Malaysia. The Taskforce discussed the next steps to move forward on implementing the eight functions of the ASEAN Regional CERT as listed:

- Facilitate coordination and information sharing between AMS National CERTs.
- Develop and maintain an ASEAN Point of Contact (POC) network of cybersecurity experts and organisations.
- Host ASEAN cybersecurity conferences/meetings, and trainings for AMS National CERTs.
- Facilitate and conduct regional cybersecurity exercises.
- Partner with other international and regional organisations in support of ASEAN cybersecurity interests and objectives.
- Develop partnerships with industry and academia.
- Support AMS National CERT capacity-building and exchange of best practices.
- Support the conduct of cybersecurity awareness campaigns in coordination with other ASEAN Sectoral Bodies related to cybersecurity and the ASEAN Cyber-Coordinating Committee.

Completion of Norms Implementation Checklist

A rules-based international order in cyberspace is essential for ensuring an open, secure, stable, and interoperable cyberspace for ASEAN region to reap socio-economic benefits in an increasingly digitalised landscape. CSA and the United Nations (UN) Office for Disarmament Affairs launched the Norms Implementation Checklist (NIC) initiative under the auspices of the UN-Singapore Cyber Programme in 2020 following ASEAN's commitment to subscribe in principle to the 11 norms of responsible State behaviour in cyberspace from the 2015 consensus report of the UN Group of Governmental Experts (UNGGE). The completed NIC was presented to ASEAN Ministers at the 9th AMCC.

The NIC comprises a set of actions that all States can consider and follow to implement the UN norms of responsible State behaviour in cyberspace. The actionable items for each norm are separated into five pillars: policy, operation, technical, legal, and diplomacy. The NIC further outlines the suggested capacity-building activities for States to consider undertaking to support them in implementing the norms.

As co-lead of the norms implementation efforts in ASEAN, Singapore, in partnership with the National Cyber Security Agency of Malaysia, and with support from the UN Institute for Disarmament Research, organised a workshop in August for AMS to finalise the NIC.

The NIC is the first regional checklist of its kind and will serve as a reference not just for AMS but for countries beyond the region to support the collective efforts to build a safer and more secure cyberspace.

AI and its impact on Private Security explained in the new CoESS Charter on the Ethical and Responsible Use of AI

What Artificial Intelligence (AI) applications are driving innovation in security and what core principles should guide the ethical use of AI in the security industry to harness its potential while mitigating its risks? These are some of the questions that the Confederation of European Security Services (CoESS) is addressing with its new Charter on the Ethical and Responsible Use of AI in the European security services – available at www.coess.eu. Launched recently, this landmark initiative provides essential guidance for security companies as they navigate the growing integration of AI systems into their operations.

Charter

on the ethical and responsible use of **Artificial Intelligence** in the European private security services

As AI technology becomes more prevalent in security services — ranging from data-driven risk analysis to smart security solutions — its potential benefits to public security and society are manifold. However, certain AI applications come with important risks. The European Union's AI Act outlines regulations for "high-risk" AI, placing new important compliance demands on businesses. Security companies must realize when they are utilizing AI in their services, they must be able to distinguish between "low-risk" vs. "high-risk" systems and use cases, and need to fully understand the implications of this legislation.

The CoESS Charter, developed by a dedicated Expert Group, aims to go well beyond ticking regulatory boxes: it champions a human-centric approach to AI innovation, rooted in a set of core values established in the document. While helping companies assess AI systems and use cases, the Charter highlights both the opportunities and challenges of AI deployment in security. It offers practical recommendations and compliance requirements for when deploying AI, including a checklist, ensuring companies navigate AI integration responsibly and effectively.

With this Charter, CoESS aims to enhance understanding of the use of AI in security solutions and underscores the commitment of its members to promoting ethical and responsible innovation in the security industry at the benefit of public security and society.

An Interview with EUSPA

Ben Lane, CIPRE event manager, met Florent Koné who currently serves as the IRIS^2 SatCom Market and Innovation Officer at EUSPA (European Union Agency for the Space Programme) where he defines strategies to drive the uptake of EU Space services for the critical infrastructure market segment.

Ben Lane (BL): Please tell us a little bit about yourself, who you are and why you are here.

Florent Koné (FK): Thank you. Good to be here. I am the IRIS^2 SatCom Market and Innovation Officer here at EUSPA, a European Union organisation I joined just over a year ago after spending more than 15 years in the private sector, mostly in the SATCOM industry with various roles ranging from technical to commercial.

Florent Kone, IRIS^2 SatCom Market and Innovation Officer at EUSPA

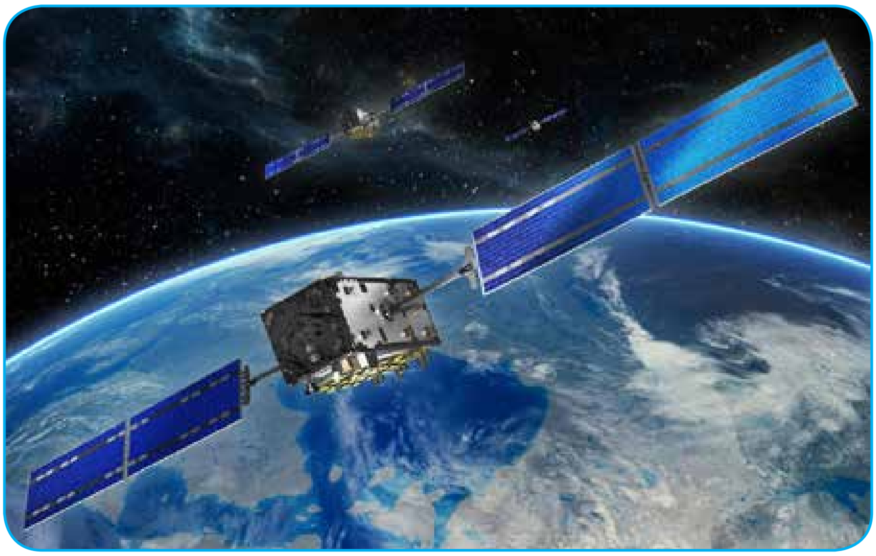
BL: Great. Thank you very much. So, first question: can you tell us a bit more about EUSPA and its roles and functions?

FK: EUSPA, the European Union Agency for the Space Programme, is the user-centric operational agency for the EU Space Programme. It was created in 2021 off the back of the proven record of its predecessor agency called GSA, the European GNSS Authority, which spearheaded the development of Galileo and

EGNOS. As the European Union expanded its space capabilities and assets, the scope and mandate of the previous agency expanded and led to the creation of a bigger agency (now called EUSPA), which has a much larger mandate. We now cover much more than the European Union satellite navigation systems. We cover three additional space components, Copernicus, which is the European earth observation program as well as secure government satellite communications components through GOVSATCOM and IRIS². The third component is a space situational awareness programme, which is critical for monitoring space hazards and space traffic.

As an operational agency, EUSPA has three main tasks; an exploitation activity, we are managing the operations of some EU space components, mostly Galileo and EGNOS and EU SST Front Desk. Then there is the operational security activity. EUSPA is ensuring the safety and security of the EU Space Programme in space and on the ground. We monitor 24/7 the security of Galileo for instance. Finally, we work to ensure there is an uptake of the EU Space programme components capabilities by the EU community of users.

BL: The second point I would like to raise with you is how does EUSPA see the EU space Programme contributing to the security of Europe's critical infrastructure?



FK: We see the EU Space Programme as a vital tool for securing Europe's critical infrastructure operations by providing reliable, secure space-based services. All the components from Galileo, EGNOS, Copernicus and GOVSATCOM offer a range of capabilities to support the protection and resilience of critical infrastructure. We can cover the full life cycle of critical infrastructure from site selection to operations and decommissioning. For example, with our Earth's observation programme, Copernicus, we can monitor land deformations, which is a key input before selecting a site for building critical infrastructure, and then we can monitor its operational life to make sure the land integrity remains safe.

Now, if I use Galileo to illustrate what we can do, when we look at complex networks; timing synchronisation is a key attribute to operate these various networks because critical infrastructure operators, such as in the energy vertical, need to understand what is happening in a specific part of the network in order to take actions in another part of the network (to ensure the energy supply matches the demand and avoid outage events). A terrestrial source of timing synchronisation is clearly possible, however, having a Galileo-based solution brings an additional layer of resilience against cyber-attacks or physical attacks; it is much more complicated to bring a satellite down than cutting a cable or attacking a terrestrial network!

BL: How is the GOVSATCOM programme contributing to European security and what can users expect from it now and in the future?

FK: GOVSATCOM will be the new kid on the block. This capability is not live, but we are getting there. By early next year, we will have initial services. GOVSATCOM will be a shift of paradigm in the way that all EU member states will be able to access secure SATCOM services. Today there is what we call a "fragmentation of the demand," which means that every member state is shopping around for SATCOM needs or building their own system. With the launch of GOVSATCOM, we will create what we call a "common EU pool." We are going to pool secure SATCOM capability, which the member states will have access to, via a dedicated platform: the GOVSATCOM hub. And this is really a big shift in how member states will be able to access and consume such services. We will create an ecosystem through this platform. There will be a centralised catalogue of services that member states and authorised users will be able to browse through. There will be monitoring capability and a help desk to support users. This upcoming capability will ease the pressure on our member states and, as importantly, increase the pace at which they can access secure SATCOM services.

BL: Okay, great. And we will be hearing more about that next week, I believe, during your presentation.

FK: Definitely.

BL: How will IRIS^2 Constellation differ from GOVSATCOM when this is introduced? What is the difference between these two components?

FK: These two components fall under the same umbrella within EUSPA and are known as Secure SATCOM. So, we have two pillars, GOVSATCOM, that we just talked about, and IRIS^2. There are fundamental differences between these two pillars. GOVSATCOM is a platform. It is a digital solution (called GOVATCOM Hub) through which users and member states will be able to browse a suite of SATCOM services based on the catalogues we build, and this catalogue of services will be built based on the existing offering from governmental SATCOM operators and commercial SATCOM operators. IRIS^2 is different and is a game changer because it will be the EU-owned constellation of SATCOM satellites. So, this constellation of SATCOM satellites will belong to the EU and will enhance the GOVSATCOM portfolio.

When IRIS^2, this constellation of satellites, is live around 2030, its capability will be available through the GOVSATCOM Hub. In short, the GOVSATCOM Hub will be a platform to access services based on the current capability from governmental and commercial operators and IRIS^2 will be an EU-owned constellation of SATCOM satellites that will be plugged into the GOVSATCOM Hub and enhance the suite of services that our member states will be able to benefit from.

BL: How is EUSPA ensuring its space programme remains secure in terms of cyber hacking, for example?

FK: I will provide two examples that are quite relevant. If we look at our longest running space component, which is Galileo, as part of this programme, when we launched the first generation of satellites and then a set of services off the back of it, everything was accredited through the SAB, the Security Accreditation Board. This board plays a pivotal role in accrediting all EU Space Programme components. It ensures the security risks are known and security measures are taken to ensure those risks are at an acceptable level. So, each time we do something in any of our EU space components, it must be vetted independently by this board, where representatives from each member state sit.

In addition, there is a security monitoring centre (GSMC) that monitors 24/7, 365 days a year what is happening around the Galileo network to ensure the safeguard of the services from this constellation. So cyber security is really embedded from day one into the operations of this system. This is what EUSPA is managing to ensure; a prominent level of cyber deterrent solutions as part of the operations of the EU space components (such as Galileo or the upcoming GOVSATCOM).

BL: Okay, that is great. Thank you, Florent, and see you in Madrid for more discussions and further details.

FK: Thank you

Critical Infrastructure Protection Week *in Europe*

International Association of CIP Professionals

14th-16th October 2025 - Brindisi, Italy

critical infrastructure PROTECTION AND RESILIENCE EUROPE

SAVE THE DATES

Securing the Inter-Connected Society

The International Association for CIP Professionals is delighted to be hosting the 2025 CIP Week in Europe with the patronage of the City of Brindisi.

The premier event for the critical infrastructure protection and resilience community, Critical Infrastructure Protection and Resilience Europe (CIPRE) brings together leading stakeholders from industry, operators, agencies and governments to collaborate on securing Europe.

CALL FOR PAPERS - Deadline 31st March 2025

The CIPRE Conference Committee are currently accepting abstracts for consideration for inclusion in the 2025 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 Brindisi, Italy for the next CIP Week in Europe and the 10th 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

With the patronage of the City of Brindisi

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

An Interview with ASD Europe

Ben Lane, CIPRE event manager, met with David Luengo, Managing Director of Indra's Brussels office, who spoke on behalf of the Aerospace, Security and Defence Industries Association of Europe (ASD), in his capacity as Chairman of the Security Business Unit (SBU) which he has headed since 2019.

ASD (www.asd-europe.org/) is the voice of the Aerospace, Security and Defence industries of Europe. With twenty-five major companies and 25 National Associations as members, the overall representation adds up to more than 4,000 companies across 21 European countries.

Ben Lane (BL): Thank you for joining us today for our 15-minute CIPRE interview. We will kick start off with the first broad question. Please provide a brief background on ASD Europe and its involvement in the critical infrastructure sector.

David Luengo, Managing Director of Indra's Brussels office

David Luengo (DL): ASD Europe is an association of national associations and prime companies that works toward achieving common objectives at the European level. The industries ASD represents are active in four sectors: civil aviation, defence, and civil security. Our companies are also involved in the space domain, which is represented by ASD's sister association Eurospace. ASD, in a nutshell , is a forum to exchange information, ideas, initiatives, and activities between technology providers across their domains of operation.

When it comes to critical infrastructure, ASD is also a place for technology providers to jointly develop their understanding of the operators' practices. As an example, digitalisation will enormously increase the interdependence of critical infrastructures. The energy sector, the transport sector, airports, ports, all the different critical infrastructures, together form the backbone of Europe's economy and society. When new digital technologies are introduced, the network gains size and density. It is critical for technology providers to understand the operational challenges these changes imply. ASD is a platform to that end, which in turns allow technology providers to better help operators.

When we talk about the security of critical infrastructures, we must consider the security of the whole network. Because operators are now much more connected across national borders , European solutions are required. Which is why ASD is trying to create common practices and to deliver solutions at a European level. Adopting a European viewpoint is vital and ASD's raison d'être.

ASD also works on how to tackle the many challenges we have ahead. In today's geopolitical context, hybrid warfare has become a reality, and the protection of critical infrastructures against hybrid threats has become essential. So, we need to put more effort into the system. This means also increased and streamlined European funding for security, and incentives for European collaboration in the field. Ultimately, ASD's purpose is to help technology providers to deliver projects which are useful for operators.

BL: Thank you – great answer, some of which we will be discussing at CIPRE 2024 in Madrid. In your opinion what are the main changes in threats against critical infrastructures that ASD and its members are seeing?

DL: In our view, the advent of hybrid threats represents the most important change. Ten years ago, the main manmade threat to critical infrastructure was terrorism. Today, we have moved into the age of hybrid warfare, where the main threat to critical infrastructure is malicious action by State or state-sponsored actors. The digital component of hybrid attacks is of particular concern, although there are also threats against physical infrastructure.

We know about the Nord Stream pipelines sabotage, or about the Russian sponsored attacks taking place across Europe. But I would say the main challenge we have today are cyber-attacks. We need a common policy on this matter, not just regulation, but also incentives to build knowledge, so we can gain better insights into different scenarios, anticipate threats more effectively, improve our threat analysis, share information to respond to those threats, and recover in case of incidents.

Finally, we must not forget that natural disasters are also increasing in frequency and scale. It is true that they have always been on our radar screen, but climate change will bring them to a completely new level that necessitates very important adaptation measures.

BL: Thank you. How are the latest NIS2 and CER directives impacting ASD members and technology providers? What is your view on this subject?

DL: If we want a balanced

level across Europe in terms of capacity, best practices and secure infrastructure, I think it is vital to have a common regulation that is put into practice by all operators. So, the NIS2 directive, in my view, must respond to the protection of common interests, the protection of consumers and the protection of operators. It's the same for the Critical Entities Resilience (CER). When investing in a network of critical infrastructures, which will be increasingly interdependent, increasingly used for public services, for the public good, then regulation is vital.

We need to update these regulations and incentivise the adoption of new systems, of new technologies, of new capacities, and knowledge. I want to see regulation as a good thing for the security market, as it urges us to think about better solutions; how to improve the service that we provide to our customers; how to improve the use of new technologies. So, this is a good thing for ASD members as technology providers. And it should be a good thing for operators of critical infrastructure.

The main point is to undertake this work collaboratively. We need to work at the European level, between operators and providers at a European level throughout the interconnected network. This means the European institutions should play a key role in helping manage the use of technology, creating collaboration, and in helping to produce better solutions.

BL: Thank you. Finally, are there any regulations or standards or even changes to standards and regulations that ASD would like to see?

DL: The way I see it, standards are a way for us all to mature the market. Standards should not block innovation, but rather help provide better and more transparent conditions to the market in terms of use, in terms of developing technologies.

During the past 10 years, the EU was successful in creating the Connecting Europe facility, for example, to provide incentives to develop trans-European networks for Energy, Transport, and the digital domain.

It is common sense to include a security layer in these existing instruments, and to develop a European security financial instrument which could support the development of this security component of the trans-European networks.

Cyber-attacks are frequent and becoming the new normal. We need to address this collaboratively. Promoting new EU incentives to tackle this security challenge is one of the key priorities.

BL: Okay, great. Throughout that interview you used the word collaboration, and this is an especially important word, particularly now. Without collaboration, nothing is going to happen effectively. Hence, the CIPRE conference in Madrid is vital because it is about collaborating, discussing, and networking with key people from across the sectors to understand how to move forward.

DL: Absolutely.

BL: Thank you

Five Eyes cyber leaders provide threat briefing

Cryptography is a set of mathematical processes that can "lock," "unlock," or authenticate information. Agencies, banks, utilities, and others rely on cryptography—e.g., data encryption algorithms—to secure systems and data.

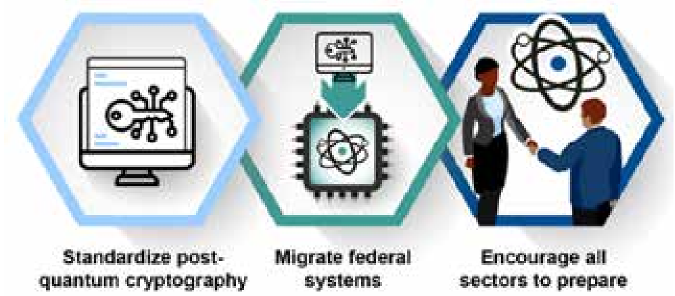
Experts predict that a quantum computer capable of breaking such cryptography may exist within 10-20 years.

Various federal entities have developed documents that inform a national strategy for addressing this threat. But the strategy lacks details and nobody's in charge of implementing it. We recommended the National Cyber Director coordinate the national strategy and use our guidelines for effective national strategies.

GAO was asked to examine the federal government's strategy to address the threat that quantum computers pose to our nation's cryptography. This report provides information on, among other things, how cryptographic methods protect systems and data, the threat quantum computers pose, and the extent to which the U.S. national quantum computing cybersecurity strategy addresses the desirable characteristics of a national strategy.

Federal agencies and the nation's critical infrastructure—such as energy, transportation systems, communications, and financial services—rely on cryptography (e.g., encryption) to protect sensitive data and systems. However, some experts predict that a quantum computer capable of breaking certain cryptography—referred to as a cryptographically relevant quantum computer (CRQC)—may be developed in the next 10 to 20 years, putting agency and critical infrastructure systems at risk. Quantum computers leverage the properties of a qubit (the quantum equivalent of classical computer bits) to solve selected problems significantly faster than classical computers.

To address this threat, various documents developed over the past eight years have contributed to an emerging U.S. national strategy. Based on its review of these documents, GAO identified three central goals.



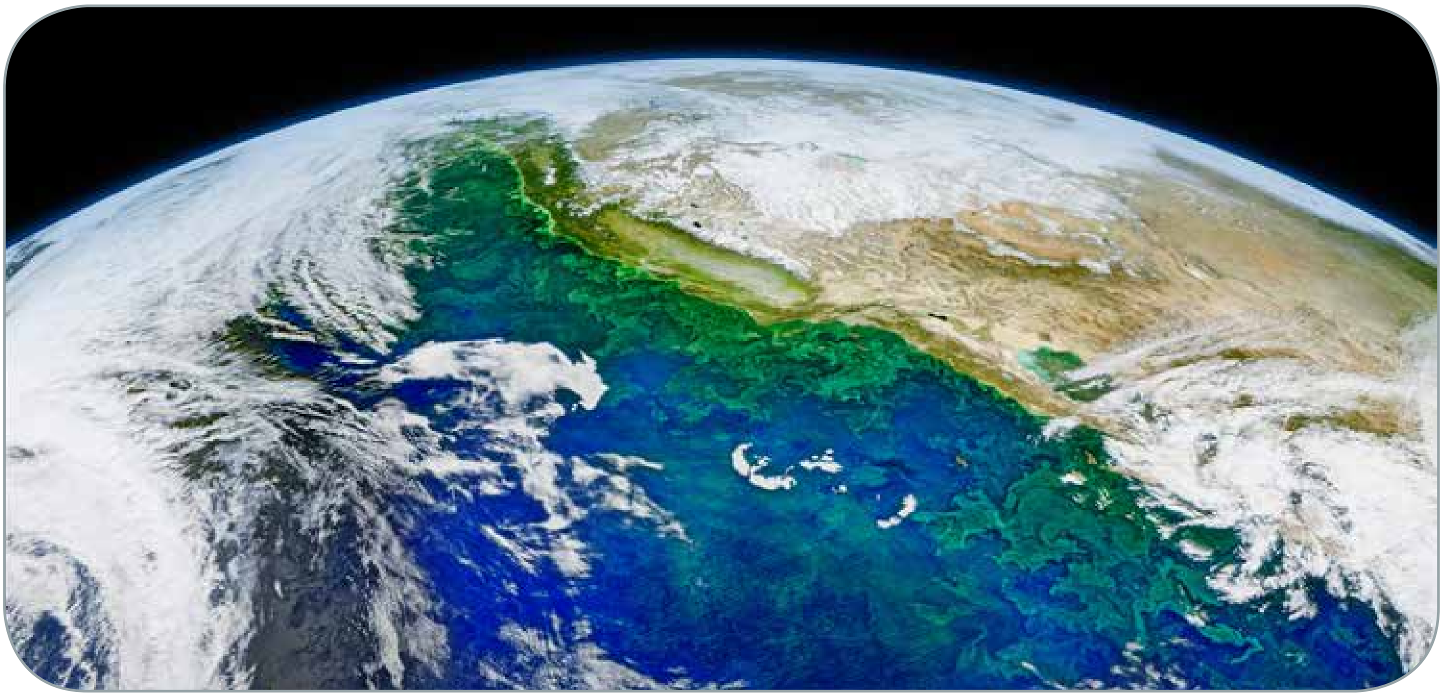
Standardize post-quantum cryptography
Migrate federal systems
Encourage all sectors to prepare

The strategy partially addresses the desirable characteristics of a national strategy identified in prior GAO work. For example:

- Problem definition and risk assessment. Several documents defined the problem as the threat of a CRQC to cryptography, but did not fully define a CRQC. In addition, although the executive branch conducted a comprehensive risk assessment on systems with vulnerable cryptography supporting critical infrastructure, it has not conducted such an assessment for systems used by federal agencies.
- Purpose, scope, and methodology. Several documents identified purpose and scope. With regard to methodology, three post-quantum cryptography standards documents provided information on how they were developed. However, the remaining documents did not describe the methodology or process used to develop them for the other two goals.
- Objectives, activities, milestones, and performance measures. The strategy documents identified objectives and activities for the first two goals but did not do so for the third. In addition, the strategy documents did not fully identify milestones for the second and third goals and did not identify performance measures for any of the three goals.

These desirable characteristics have not been fully addressed, in part, because no single federal organization is responsible for coordinating the strategy. In January 2021, Congress established an organization that is well-positioned to lead these efforts: the Office of the National Cyber Director. If the office embraces this role and ensures that the strategy fully addresses the desirable characteristics, the nation will have a better-defined roadmap for allocating resources and holding participants accountable.

Weather Ready Pacific charts the way on Early Warnings for All



Weather Ready Pacific - a major ten-year programme – aims at reducing the human and economic cost of severe weather events, protecting Pacific Island communities and livelihoods on the frontline of climate change.

WMO Deputy Secretary-General Ko Barrett stressed WMO's commitment to the initiative in a high-level event at COO29 on "Early Warnings For All in the Pacific: Starting our journey to navigate through the challenges of a climate change world."

Ministers and their representatives from Tonga, Fiji and Samoa highlighted the importance of the programme in building resilience to hazards such as tropical cyclones and coastal inundation in an era of rising sea levels and more extreme events.

Tiofilusi Tiuete, Minister for Finance and National Planning of Tonga, said there were already tangible improvements in forecasts thanks to a new weather radar which will increase the accuracy of advance warnings of high-impact events.

The Weather Ready Pacific Program was developed with the support of the Secretariat of the Pacific Regional Environment Programme (SPREP), WMO and the Government of Australia through the Australian Bureau of Meteorology (BOM). It is administered by SPREP and has a target to raise US $ 191 million over 10 years to strengthen the capacity of National Meteorological and Hydrological Services in the Pacific.

"We are committed to supporting

sustainable capacity enhancement efforts wherever they occur and we stand ready to support with technical tools and guidance. National Meteorological and Hydrological Services are at the centre of all these efforts," Ko Barrett told the high-level event.

"We are happy to leverage funding through the Systematic Observations Financing Facility (SOFF) and the Climate Risk and Early Warning Systems Initiative (CREWS) and other investment instruments to support the aims of the Weather Ready Pacific Programme and more generally of the Early Warnings for All initiative."

Climate change ambassadors from Australia and New Zealand, two of the main financial backers, stressed how the programme is intended to foster long-term investment in sustainability. The aim is to bring different funding initiatives from a variety of partners under one roof and within a 10-year time frame, thus easing the administrative burden on Small Island Developing States.

"We have had so many projects that stop and start, stop and start. We spent more time writing reports than we do forecasting the weather," said 'Ofa Fa' Anunu, the coordinator of the Weather Ready Pacific Programme. He was formerly the head of Tonga's NMHS and president of WMO's Regional Association for Asia-Pacific.

Systematic Observation Financing Facility (SOFF)

The Pacific represents 15 % of the world surface, but it has only six upper air stations which are compliant with the Global Basic Observing Network. This is a major gap that needs to be filled, given that a chain is only as strong as its weakest link.

A geodesic dome-shaped weather radar tower stands on a metal framework against a background of blue sky and clouds. Logos are visible on the dome's surface.

SOFF seeks to fill this gap through long-term, grant based investments in infrastructure and enhancing the capacity of National Meteorological and Hydrological Services (NMHS).

Within the Pacific, Kiribati and the Solomon Islands have been approved for an amount of USD 20 million. Nauru and Samoa have been provisionally approved for an amount of USD 12 million.

Climate Risk and Early Warning Systems Initiative

Climate Risk and Early Warning Systems initiative seeks to bridge the early warnings capacity gap. Ko Barrett said CREWS is a textbook example of people-centred, community-based projects that are making a tangible difference to people's lives.

WRP and CREWS share common programming frame and principles of country/regional driven programmes, people-centered approaches, and gender-responsiveness, said Gerard Howe, Head of Energy, Climate and Environment Directorate, UK Foreign, Commonwealth and Development Office (FCDO) and Chair of CREWS.

"CREWS is committed to support Weather Ready Pacific as a vehicle for more effective programming and financing," he said.

Pacific Island countries benefited from one of the very first CREWS financing decisions in 2017. The CREWS Steering Committee recently initiated the consultations for a third phase of this regional project bringing the total contribution to the region to USD 25 million.

In Papua New Guinea, with the support of the Australian meteorological services, a new drought early warning system was established. In PNG, nearly eight in ten people rely on subsistence farming. Food insecurity is mostly

due to crop failures from drought and frost.

Support to develop similar drought advisories has been received from 5 additional Island States and an additional US$ 5 million committed to support these.

Two countries (Tonga and Vanuatu) have accessed financing through the CREWS Accelerated Support Window a fast-track provider of technical assistance. This has led to the development of a smart weather app.

International Cooperation Strengthens Global Infrastructure

S&T has a mandate to work across the Department of Homeland Security's (DHS) mission spaces to identify opportunities to leverage science and technology to tackle not only the challenges of today, but also those waiting just over the horizon. In 2004, when S&T was in its early days, the Directorate recognized the value of international research and development (R&D) partnerships to accomplish this mandate—because we know that the biggest challenges are not ones that we face alone, and they are not ours to overcome alone.

The first two official international agreements S&T signed were with Canada and the United Kingdom (UK), and this year we celebrated 20 years of incredible accomplishments with both partners. From cross-border search and rescue (with some early artificial intelligence!) efforts with Canada to a long history of protecting the traveling public with the United Kingdom (UK), our respective nations, our first responders, our citizens, and the world are all safer because of these relationships.

Few areas capture this interconnectedness like protecting our critical infrastructure. In addition to joining forces with our domestic partners—across DHS and other federal agencies, as well as our state and local counterparts—we also work closely with all our international partners to harness innovation.

Any differences we may face in our respective contexts become assets that contribute to more robust technology solutions to protect our frontline operators and communities.

One example of such collaboration is Transportation Systems Sector: Industry Innovation with the UK

Since 2007, S&T has partnered with the UK to participate in the Innovation Research Call (IRC), a multi-million dollar competition to find state-of-the-art technological solutions for the improved detection of explosives and weapons. IRC has launched several commercially available products used in airports and other locations. By joining with the UK on this initiative, S&T is able to access and operationalize innovations from international industry and ensure our mission needs are being addressed on a broad scale—improving the safety of airports and public spaces not only in the US, but across the world.

Using satellite sea level tracking to anticipate storms and protect coastal areas

The ongoing 2024 Atlantic hurricane season is leaving a lasting footprint due to the resulting fatalities and infrastructure damage in coastal zones. Timely forecasts of extreme sea levels are crucial to mitigate the imminent risk that challenges the capacity of emergency response systems.

Hurricane Beryl, on which Copernicus prepared emergency maps, made history as the earliest Category 5 Atlantic hurricane on record. Category 4 Hurricanes Helene and Kirk along with Category 5 Hurricane Milton resulted in an aftermath totalling over 264 fatalities and costing $172 billion in damage.

As a result, forecasting where and when natural disasters are likely to occur is critical, and satellite measurements, with their global ocean coverage, can be key to making these forecasts more accurate.

Satellites can provide information about the sea level across the world's oceans, despite their temporal scarcity due to the long and variable revisit times of each satellite mission.

Aiming to overcome this limitation, which is important for identifying extreme episodic sea levels, the Joint Research Centre, CEDEFOP, LEGOS (France), and USC (USA) conducted an analysis relying only on publicly available satellite-derived measurements from 23 missions - including those from the Copernicus Contributing Missions.

The analysis led to a continuous in-time description of the open ocean sea level for a period of 63 years, revealing both the areas of the general circulation ocean currents and the areas exposed to intense tropical cyclone activity.

Improving sea level prediction to better protect coasts

The efficacy of the proposed methodology for real-time sea level forecasts was demonstrated by estimating the sea level triggered by Tropical Cyclone Kong-rey – the most powerful tropical cyclone worldwide in 2018.

Using 51 atmospheric forecast scenarios and the satellite data-driven model, the researchers estimated both with high accuracy and high likelihood the tropical cyclone-induced peak sea level and footprint on the sea surface, three days before it made landfall in Japan.

New guide to help manage risks from technological accidents triggered by natural hazards

OECD, the UN Economic Commission for Europe (UNECE) and the JRC have joined forces to develop a guidance to inform senior leaders in industry and public authorities of Natech risk and to support them in setting direction for implementing respective risk reduction measures, including the integration of Natech risk management into corporate governance strategies and national policies.

Senior leaders in industry and public authorities have a critical role to play in ensuring the appropriate delivery and governance of Natech risks, especially in a changing risk landscape due to climate change. Awareness raising, active engagement and informed decision-making can facilitate effective Natech risk management.

The guide provides recommendations for action on risk awareness and risk governance, prevention, preparedness and response to Natech accidents, communication among industry, public authorities and beyond, leadership of a multidisciplinary team, and international and transboundary considerations. The guide also includes self-assessment checklists that should help senior leaders to gauge how prepared their organisation is in managing Natech risk effectively.

NCSC warns of widening gap between cyber threats and defence capabilities

The UK's cyber security chief is urging allies and partners to join forces and close the widening gap between escalating cyber threats and our collective ability to defend against them.

Speaking at Singapore International Cyber Week, Dr Richard Horne, the newly appointed head of GCHQ's National Cyber Security Centre (NCSC), called for greater global resilience in the face of increasingly complex and aggressive online security threats. He said:

"Increased dependence on technology is driving growth and transforming societies, creating exciting new opportunities. It also exposes us to greater cyber risks. Without collective action, we risk widening the gap between the escalating threats to our societies, critical services, and businesses, and our ability to defend and be resilient.

"The threat landscape is growing more complex, with significant incidents on the rise. To close this gap, we need coordinated global efforts to strengthen cyber resilience, ensure security is built into technology from the outset, and prepare both the public and private sectors to not only defend but also recover swiftly from destructive cyber attacks."

Dr Horne also highlighted that the rapid expansion of cyber capabilities – previously confined to nation-states and well-resourced actors – has significantly broadened the threat landscape. In 2024, the NCSC has already responded to 50% more nationally significant incidents compared to last year, as well as a threefold increase in severe incidents.

Responding to questions about these capabilities and their use in ransomware attacks, Dr Horne said:

"The data confirms why global collaboration is more critical than ever. The Counter Ransomware Initiative is a perfect example of this, and I am very proud to work alongside our friends and hosts in Singapore to make it a success.

"Last month, 39 nations and eight international insurance bodies endorsed guidelines for organisations navigating ransomware payments. This is a prime example of the progress we can achieve by working together, proving that cyberspace knows no boundaries."

Elsewhere, Dr Horne emphasised the importance of long-term technology resilience, warning that many innovations could become vulnerable without integrated management and security over the lifetime of the product. He urged developers to plan for the future and ensure that today's technology can withstand tomorrow's cyber threats.

"Today's innovation is tomorrow's legacy. The innovative technologies we are building today will become the legacy technologies of tomorrow. We must adopt a lifecycle management approach to ensure they remain secure and resilient in the future.

"This is a task that businesses and public services cannot tackle alone. Governments must step in to set the tone and guide the conversation."

UK and allies warn about shift in cyber attackers exploiting zero-day vulnerabilities

In a new advisory, the National Cyber Security Centre (NCSC) – a part of GCHQ – alongside partners in Australia, Canada, New Zealand and the United States, shared a list of the top 15 routinely exploited vulnerabilities of 2023.

Of these vulnerabilities, the majority were first exploited as zero-days – weaknesses that were recently discovered and where a fix or patch was not immediately available from the vendor – allowing attackers to conduct cyber operations against higher-priority targets.

This trend, which the NCSC has continued to observe into 2024, marks a shift from 2022 when less than half of the top list was initially exploited as zero-day vulnerabilities.

The advisory strongly encourages enterprise network defenders to maintain vigilance with their vulnerability management processes, including applying all security updates in a timely manner and ensuring they have identified all assets in their estates.

Joint Statement from FBI and CISA on the People's Republic of China (PRC) Targeting of Commercial Telecommunications Infrastructure

The U.S. government's continued investigation into the People's Republic of China (PRC) targeting of commercial telecommunications infrastructure has revealed a broad and significant cyber espionage campaign.

Specifically, we have identified that PRC-affiliated actors have compromised networks at multiple telecommunications companies to enable the theft of customer call records data, the compromise of private communications of a limited number of individuals who are primarily involved in government or political activity, and the copying of certain information that was subject to U.S. law enforcement requests pursuant to court orders. We expect our understanding of these compromises to grow as the investigation continues.

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) continue to render technical assistance, rapidly share information to assist other potential victims, and work to strengthen cyber defenses across the commercial communications sector.

New Resilient Power Guidance Added to the CISA Resilient Toolkit Portal

Major power outages from disasters or manmade events can substantially exacerbate emergency response operations. This can jeopardize the health and safety of personnel and substantially increase property damage. It is imperative that critical facilities and sites continue to operate during power outages to provide essential services to the population and to support the recovery effort. Any electrical grid outage can have cascading effects, and force critical facilities to rely on their own backup power generation (if they have it) and energy storage capabilities to maintain mission effectiveness for an extended period of time.

CISA recently released the Ten Steps to Resilient Power to help emergency and business continuity managers implement the Resilient Power Best Practices for Critical Facilities and Sites (RPBP). The RPBP provides guidelines, analysis, background material, and references to improve mission resilience through the use of backup and emergency power systems during power outages. This can help the nation reduce risks to, and strengthen resilience of, America's critical infrastructure.

The Ten Steps is the newest addition to CISA's Public Safety Communications and Cyber Resiliency Toolkit. Together, the Ten Steps and the RPBP help continuity managers create a comprehensive, risk-informed Business Continuity and Continuity of Operations resilient power plan to ensure their facilities are resilient and mission ready.

The target audience for the Ten Steps includes executives, chief engineers, emergency preparedness and continuity planning personnel, and those involved with cybersecurity, physical security, telecommunications, information technology, and procurement, including contractors and vendors.

The first step with any major threat to operations is understanding risk and capabilities to mitigate that risk. This guide was developed with resilience in mind for any facility size or mission scope. If you are part of a local government, a healthcare or communications provider, or an owner or operator of any type of critical infrastructure, this tool is for you.

TSA announces proposed rule that would require the establishment of pipeline and railroad cyber risk management programs

The Transportation Security Administration (TSA) published a Notice of Proposed Rulemaking that proposes to mandate cyber risk management and reporting requirements for certain surface transportation owners and operators.

"TSA has collaborated closely with its industry partners to increase the cybersecurity resilience of the nation's critical transportation infrastructure," said TSA Administrator David Pekoske. "The requirements in the proposed rule seek to build on this collaborative effort and further strengthen the cybersecurity posture of surface transportation stakeholders. We look forward to industry and public input on this proposed regulation."

This rule proposes to continue TSA's commitment to performance-based requirements. Building on the performance-based cybersecurity requirements TSA previously issued via annual Security Directives since 2021, the proposed rule leverages the cybersecurity framework developed by the National Institute of Standards and Technology and the cross-sector cybersecurity performance goals developed by the Cybersecurity and Infrastructure Security Agency (CISA).

Consistent with these requirements and standards, this rule proposes:

- To require that certain pipeline, freight railroad, passenger railroad and rail transit owner/operators with higher cybersecurity risk profiles establish and maintain a comprehensive cyber risk management program;

- To require these owner/operators, and higher-risk bus-only public transportation and over-the-road bus owner/operators, currently required to report significant physical security concerns to TSA to report cybersecurity incidents to CISA; and

- To extend to higher-risk pipeline owner/operators TSA's current requirements for rail and higher-risk bus operations to designate a physical security coordinator and report significant physical security concerns to TSA.

TSA asserts that maintaining an effective cybersecurity posture is critically important to ensuring that the surface transportation sector is prepared for, and able to manage, cyber risks. The requirements contained in this proposed rule would strengthen cybersecurity resilience across the surface transportation systems sector.

TSA intercepted 9 firearms in 30 days at Detroit Metropolitan Airport

Transportation Security Administration (TSA) officers intercepted a firearm at Detroit Metropolitan Airport (DTW) on Friday, the ninth detected in 30 days at the airport.

Including the firearm detected Friday, two have been stopped so far in the month of November. TSA officers also detected seven firearms at DTW checkpoints between the dates of Oct. 9 and Oct. 30. A total of 55 firearms have been stopped at DTW this year.

In all firearm detections at DTW, the Wayne County Airport Police were alerted, responded to the checkpoint, and confiscated the weapon.

DOE Announces Framework for Assessing Research, Technology, and Economic Security (RTES) Risk

A new memo published by the Department of Energy (DOE) outlines DOE's approach to Research Technology and Economic Security (RTES) risk for financial assistance and loan activities. The memo includes an overview of DOE's goals, process, high-level risk factors, and commitment to mitigation.

This framework codifies a harmonized approach across all DOE/NNSA funding offices, while also ensuring right-sized requirements for early-stage Research and Development (R&D) in the academic setting, applied R&D stage projects, and Demonstration and Deployment (D&D) stage projects.

To assist the applicant and recipient community in understanding and adapting to the recently published framework, DOE will provide webinars to introduce the approach and answer questions. In the coming months, DOE intends to publish additional resources that build on this framework. Once those subsequent resources are released, DOE will schedule listening sessions to gather feedback from the community. The Department recognizes that risk factors will change over time, as DOE adapts to changes in the geopolitical landscape, evolving congressional requirements, and community input.

Help2Protect against the Insider Threat

Insider Threat Awareness and Program Development Training platform

In Collaboration with:

International Association of CIP Professionals

See below for 20% Off Special Offer

THREE TYPES OF INSIDERS - ONE TOOL TO DETECT THEM

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

BE PROACTIVE

AWARENESS TRAINING

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

BE READY

PROGRAM DEVELOPMENT TRAINING

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

An eLearning Platform dedicated to Security and the Insider Threat

www.help2protect.info

SPECIAL OFFER FOR IACIPP – 20% DISCOUNT OFF THE COURSE

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

Register at: www.cip-association.org/help2protect - Promo Code: 7UATQW7M

2024 State of Healthcare Security Report From HID®: Digital and Physical Security Integration is Critical for 77% of Respondents

HID®, a worldwide leader in trusted identity solutions, has released its State of Healthcare Security Report based on input from more than 200 security and IT professionals working in a broad range of healthcare facilities.

The State of Healthcare Security Report delves into the core concerns for the healthcare industry and upcoming innovations and technologies that address them. The survey uncovers seven themes, as follows:

Healthcare's Surge in Both Cyber and Physical Security Attacks Instances of ransomware attacks on the healthcare sector have almost doubled according to The Office of the Director of National Intelligence. Additionally, a staggering 80% of nurses have encountered workplace violence within the past year according to National Nurses United, a prominent national union of registered nurses.

Notable 77% of Participants Believe it is Critical for Healthcare Facilities to Achieve Digital and Physical Security Integration Survey respondents believe that it is important for their facilities to achieve digital and physical security integration to fight the dramatic increase in cyber and physical security attacks.

Evolving Security Practices: From Physical to Digital Identity Management Conventional physical approaches such as ID badges are progressively being complemented, or in certain instances, replaced, by digital credentials such as mobile and biometric authentication. The survey indicates that 32% of healthcare facilities implement biometric authentication.

The full report includes additional data and analysis.

Airbus Protect signed a strategic partnership with EGIS

Airbus Protect, a subsidiary of Airbus delivering expertise in cybersecurity, safety and sustainability, and Egis, a leading global consulting, construction engineering and operating firm across every aspect of transport, infrastructure and the built environment, signed a strategic cooperation agreement.

This partnership will enable both companies to deliver combined cutting-edge offerings for large industrial customers with critical processes, namely air transport, rail, power generation and the automotive industry in France, the European Union and the United Kingdom.

By joining complementary forces, Airbus Protect and Egis will leverage their respective expertise to deliver innovative solutions that go beyond conventional standards, ensuring enhanced protection and resilience for our clients at every level over the entire life cycle of a product.

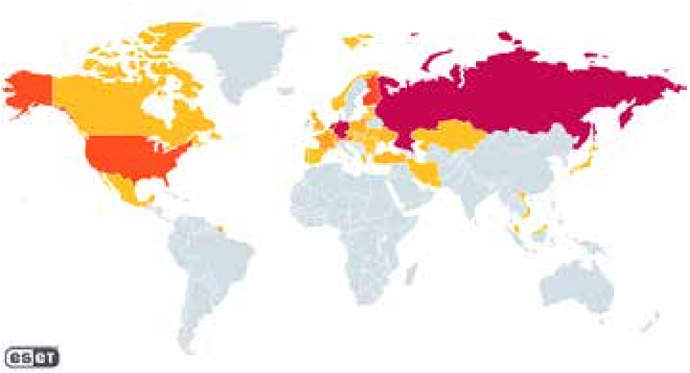
On the Airbus Protect side, it confirms a strategy focusing on comprehensive risk management, enabling industries to easily find a reliable partner to tackle risks stemming both from simple, unintentional incidents or from complex, organised attacks.

On the Egis side, this partnership demonstrates a commitment to answering a strong market demand for an engineering approach that takes major risks into account early on, making sure that assets and infrastructure are always protected.

"This partnership is an obvious step for us: our customers need a combined offering to guarantee their protection and increase their overall resilience, and with Egis we share the same culture of engineering excellence." commented Thierry Racaud, Airbus Protect CEO.

Days after takedown, ESET Research releases analysis of RedLine Stealer infostealer empire

In Operation Magnus just days ago, Dutch National police, alongside the FBI, Eurojust, and several other law enforcement organisations, performed a takedown of the infamous RedLine Stealer.

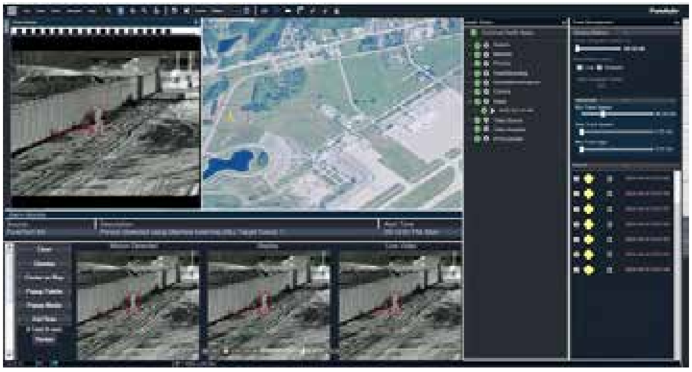


Following the takedown of RedLine Stealer by international authorities, ESET researchers are publicly releasing their research into this infostealer's undocumented backend modules.
The in-depth technical analysis provides a greater understanding of the inner workings of this malware-as-a-service (MaaS) empire. ESET researchers, in collaboration with law enforcement, collected multiple modules used to run the infrastructure behind RedLine Stealer in 2023. The Dutch National police, alongside the FBI, Eurojust, and several other law enforcement organisations, performed a takedown of the infamous RedLine Stealer operation and its clone called META Stealer on October 24, 2024. This global effort, named Operation Magnus, resulted in the takedown of three servers in the Netherlands, the seizure of two domains, two people being taken into custody in Belgium, and the unsealing of charges against one of the alleged perpetrators in the United States.

Back in April 2023, ESET participated in a partial disruption operation of the RedLine malware, which consisted of the removal of several GitHub repositories used as dead-drop resolvers for the malware's control panel. Around that time, ESET Research investigated previously undocumented backend modules of this malware family in collaboration with fellow researchers at Flare. These modules don't interact directly with the malware, but rather handle authentication and provide functionality for the control panel.

PureTech Systems Announces the Release of PureActiv® Version 16, Featuring Enhanced Geospatial AI-Boosted Video Analytics for Critical Infrastructure Protection

PureTech Systems Inc. has released PureActiv® Version 16, which introduces advanced features aimed at providing nuisance alarm elimination, and autonomous perimeter detection, classification, tracking, alerting, and deterrence—designed to address the evolving security needs of critical infrastructure.



PureActiv® Version 16 leverages PureTech's patented geospatial AI-boosted technology, delivering accuracy in detecting and classifying potential threats with near-zero nuisance alarms. One of the new capabilities in Version 16 includes enhanced machine learning (ML) models that significantly improve classification accuracy, allowing for precise differentiation between real access control events and faulty door switches/locks.

"We are excited to release PureActiv® Version 16 as the next step in autonomous perimeter security," said Larry Bowe, CEO of PureTech Systems Inc. "With enhanced machine learning models, advanced PTZ camera tracking, and integrated detection capabilities, PureActiv® continues to set the standard for protecting borders and critical infrastructures."

"This new release enables new autonomous capabilities that go beyond conventional measures, providing operational advantages and seamlessly blending with other integrated technology systems," says Chris Sincock, VP of Critical Infrastructure.

SpiderOak Releases Open-Source Project to Advance Cyber Protections for Commercial and Defense

SpiderOak, the leader in zero-trust cybersecurity solutions for next-generation space and tactical edge operations, today announced the release of their core technology platform as an open-source offering.

The project is called "Aranya" and offers the same protections as the companies OrbitSecure platform currently deployed within the Department of Defense. Now technology manufacturers will be able to embed and extend these same zero-trust protections natively into their own systems, while offering contributions to advance cyber protections and accelerate secure by design adoption recently advocated by the European Union and the Cybersecurity and Infrastructure Security Agency.

The Aranya project represents an inflection point for how cyber protections can be applied against ever increasing and sophisticated AI assisted attacks using malware, ransomware, command injection, and spoofing techniques. By transitioning protections typically enforced by vulnerable centralized security solutions and network controls to the technology manufacturers' applications and devices themselves, end user organizations will see significant reductions in cost, complexity, and their overall attack surface. With this secure by design approach, technology providers from any industry can use Aranya to embed protections to ensure every message is authentic, authorized and protected between applications, machines, and devices.

"Cybersecurity is the single greatest challenge for distributed systems with very complex architectures, especially in defense," said Charles Beames, Executive Chairman of SpiderOak.

Office of the Director of National Intelligence Selects Censys to Provide Internet Intelligence Platform™ to US Intelligence Agencies

Censys, the leading Internet Intelligence Platform for Threat Hunting and Attack Surface Management, today announced the company was awarded a multi-year contract by the Office of the Director of National Intelligence (ODNI) Cyber Threat Intelligence Integration Center (CTIIC) to provide its leading intelligence platform to U.S. intelligence agencies.

Under the Sentinel Horizon contract, Censys will provide U.S. intelligence agencies access to Censys' continuous scanning and coverage of all internet-facing assets across the globe, helping governments identify, manage and mitigate potential risks in real time. The Censys dataset is one of the most comprehensive in the industry, discovering and monitoring over 560 million new assets daily. This monitoring allows for the rapid identification of vulnerabilities and threats, ensuring that no internet-exposed device goes unnoticed or unprotected.

Studies show that over 30% of all breaches are linked to unknown or poorly managed internet-facing assets. Government agencies are particularly vulnerable, as they often manage large, complex networks with limited visibility into their full digital footprint. Censys addresses the challenges presented by the growing number of internet-exposed assets, which pose significant risks to national security and critical infrastructure.

The market for Internet Intelligence and cybersecurity is rapidly expanding, driven by the increasing number of cyber threats and the need for better visibility into internet-facing assets.

Critical Infrastructure Protection Week in Europe
14th-16th October 2025 - Brindisi, Italy
International Association of CIP Professionals

critical infrastructure
PROTECTION AND
RESILIENCE EUROPE

ADVERTISING SALES

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

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

critical infrastructure PROTECTION AND RESILIENCE N. AMERICA

March 11th-13th, 2025

HOUSTON, TEXAS, USA

A Homeland Security Event

Are you sure your national infrastructure is secure?

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

Invitation to Attend

Register online today and save with Early Bird Discounts

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

The Biden Administration rolled out a new critical infrastructure memorandum, titled National Security Memorandum on Critical Infrastructure Security and Resilience (NSM-22) which is intended to set forth the role of the federal government, including responsibilities for specific federal agencies, in protecting U.S. critical infrastructure.

NSM-22 serves to supplant PPD-21, formally known as the Presidential Policy Directive – Critical Infrastructure Security and Resilience (pdf). PPD-21, a memorandum issued during the Obama Administration, designated 16 critical infrastructure sectors that will be subject to additional oversight through the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).

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

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

Register today for Early Bird Savings on delegate fees.

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

Co-Hosted by:

International Association of CIP Professionals

INFRAGARD MEMBERS ALLIANCE HOUSTON

Speakers include:

- David Carroll, Associate Director for Mission Engineering, CISA
- Brannan Villee, Strategic Program Manager, Department of Homeland Security, Science & Technology Directorate
- Norman Speicher, Program Manager, Department of Homeland Security, Science and Technology Directorate
- Faye Francy, Executive Director, Automotive Information Sharing and Analysis Center (Auto-ISAC)
- Clint Ladd, Critical Infrastructure Protection Coordinator, Texas Department of Public Safety / Texas Office of Homeland Security
- Annie Hunziker Boyer, Chief, Chemical Security Policy, Rulemaking, and Engagement Branch, CISA
- Marco Ayala, President, Houston InfraGard Members Alliance
- Lt. Col. Tommy Waller, USMC Ret., President & CEO, Center for Security Policy, USA

For full speaker line up visit www.ciprna-expo.com/speakers2025

To discuss exhibiting and sponsorship opportunities contact:

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 270 820

The premier discussion for securing America's critical infrastructure

Supporting Organisations:

International Association of CIP Professionals

INFRAGARD MEMBERS ALLIANCE LOUISIANA

Help2Protect

STIME

ISIO - International Security Industry Organization

Executive Sponsors:

TIA

AUTO-ISAC

INSTITUTE FOR HOMELAND SECURITY

Flagship Media Partner:

critical infrastructure PROTECTION AND RESILIENCE NEWS