



Institute for Homeland Security

MARITIME RISK SYMPOSIUM 2026

Official Proceedings



Table of Content

Executive Director Letter	3
Thank You to Our Partners	4
Agenda	5
Symposium Takeaways	7
Private-Public-Academic Partnerships	
Two Day Executive Summary	
Session Observations	
Spotlight Speakers: Future-Focused Risk Management	
Day 1 – Panels	
Day 2 – Panels	
Closing Discussion	
Overall Event Readout	
Cross-Cutting Takeaways	
Suggested Next-Year Work Products	
Appendix A: One Drive Links to Conference Materials	18
Symposium Takeaways: Links for Session Videos	19

WELCOME

MARITIME RISK SYMPOSIUM

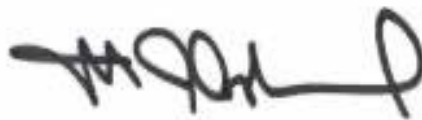
Institute for Homeland Security

Thank you for attending the 2026 Maritime Risk Symposium! We were honored to have you join us for two days of insightful dialogue, collaboration, and forward-thinking perspectives on the challenges and opportunities facing today's Maritime leaders.

This year's theme, "Overcoming Maritime Vulnerabilities Through Private-Public-Academic Partnerships", invited us to look beyond traditional approaches to security management and explore new ways to strengthen resilience, enhance leadership, and drive meaningful performance in an ever-evolving threat environment.

Our distinguished panelists and speakers brought decades of experience from across the public and private sectors. Together, they examined how innovation, partnership, and informed decision-making can empower organizations to adapt, recover, and thrive.

We hope the sessions inspired you to rethink conventional boundaries, challenge assumptions, and make lasting connections with peers who share your commitment to protecting and advancing the nation's most vital assets. Thank you for being part of this year's symposium and for your ongoing leadership in the Maritime field!



Michael Aspland, Executive Director
Institute for Homeland Security

THANK YOU TO OUR
SUPPORTING PARTNERS

Google Cloud

Security

ECHODYNE



Deloitte.



AGENDA

Overcoming Maritime Vulnerabilities Through Private-Public-Academic Partnerships

Day One - June 2, 2026

LyondellBasell Center for Petrochemical, Energy, & Technology at San Jacinto College

Focus: Maritime Cybersecurity and Artificial Intelligence

Description: This high-level discussion explores the rapidly evolving cyber risk landscape shaping the maritime ecosystem. Against the backdrop of heightened geopolitical tensions and new USCG cybersecurity mandates, regulators and industry leaders convene to share insights from the first year of compliance, examine emerging OT and AI-driven threats, and discuss strategies for strengthening resilience across ports, vessels, and supply chains.

Outcomes: Align policy, technology, and operations to safeguard critical maritime infrastructure while ensuring the continuity and competitiveness of U.S. commerce.

7:00AM – 8:15AM	Conference Registration with Refreshments Provided
8:15AM – 9:00AM	Opening: Day One - Welcome / Safety Brief / Framing the Conference
9:00AM – 10:20AM	Introduction / Keynotes
10:20AM – 10:30AM	Break / Networking
10:30AM – 11:20AM	Cyber Intel Threat Brief
11:20AM – 11:30AM	Break / Networking
11:30AM – 12:20PM	Panel: Navigating the New Normal: USCG Cyber Rules & Industrial Reality
12:20PM – 1:20PM	Working Lunch Program Panel: Cyber / Physical Control Systems Title: Securing the Converged OT/IT Environment
1:20PM – 1:30PM	Break / Networking
1:30PM – 2:20PM	Panel: Artificial Intelligence Title: Guardians of the Guardrails: Securing Artificial Intelligence in Maritime Operations
2:20PM – 2:30PM	Break / Networking
2:30PM – 3:20PM	Panel: Risk Assessment / Analysis Title: Charting the Unknown: From Asset Discovery to Strategic Resilience
3:20PM – 3:30PM	Break / Networking
3:30PM – 4:20PM	Panel: Putting it All Together Title: The Captain's Watch: Operationalizing Cyber Resilience
4:20PM – 4:50PM	Student Poster Contest Announcement Sponsored by Rutgers University
4:50PM – 5:00PM	Wrap Up: Day One

AGENDA

Overcoming Maritime Vulnerabilities Through Private-Public-Academic Partnerships

Day Two - June 3, 2026

LyondellBasell Center for Petrochemical, Energy, & Technology at San Jacinto College

Focus: Maritime Cybersecurity and Artificial Intelligence

Description: A strategic discussion examining how disruptions in littoral maritime environments—across ports, coastal infrastructure, border security, technology systems, shipbuilding, and supply chains—create cascading risks to private industry and national security, and how integrated private-public-academic solutions can strengthen economic resilience and maritime readiness.

Outcome: Align industry, academia, and government on actionable strategies that enhance maritime security, technological integration, supply chain stability, and workforce capacity to mitigate economic and security risks in the coastal and near-shore domain.

7:00AM – 8:15AM	Conference Registration with Refreshments Provided
8:15AM – 8:20AM	Opening: Day Two
8:20AM – 9:30AM	Panel: Forging Maritime Readiness through U.S. Shipbuilding, Supply Chains, and Workforce
9:30AM – 9:40AM	Break / Networking
9:40AM – 10:50AM	Panel: Littoral Disruptions and Cascading Consequences on Private Industry
10:50AM – 11:00AM	Break / Networking
11:00AM – 12:10PM	Panel: Maritime Border Security
12:10PM – 1:30PM	Working Lunch Program Panel/Demo: Addressing Elements of Maritime Risk from The Sky
1:30PM – 1:40PM	Break / Networking
1:40PM – 2:40PM	Panel: Harbor Safety and Security Committees: A Case Study
2:40PM – 3:20PM	Wrap Up: Day Two To prepare for MRS2027, What are the Actions that need to be taken by industry and academia over the next year?
3:20PM – 3:30PM	Closing – MRS2026 Co-Chairs



Symposium Takeaways

Private-Public-Academic Partnerships

MRS2026 did what a strong symposium should do: it connected strategic risk to operational work. The event brought maritime, energy, cyber, port, law enforcement, academic, and industry leaders into one conversation and kept returning to a practical question: how do we keep the maritime system moving when the disruption is cyber, physical, autonomous, geopolitical, or all the above? The Houston setting made that question concrete. Speakers repeatedly framed the Houston Ship Channel as an economic engine whose interruption would ripple quickly through energy, manufacturing, transportation, and communities.

Two Day Executive Summary

Day One built a common picture of cyber and AI risk. The discussion moved from the strategic threat landscape to Coast Guard cyber rules, IT/OT convergence, AI guardrails, asset discovery, supply-chain risk, and incident response. The strongest message was that plans and compliance are necessary but not sufficient. Operators need exercised decision rights, good asset visibility, tested backup procedures, clean vendor escalation paths, and senior leaders who know what information they need in the first hour of an incident.

Day Two widened the lens to shipbuilding, littoral disruption, maritime border security, drone/radar awareness, and port partnerships. The dominant theme was cascade: maritime disruptions rarely stay maritime. It crosses ports, vessels, trucking, rail, power, telecom, insurance, workforce, public safety, military readiness, and local economies. The center of gravity for MRS2027 should therefore be progress, not another conversation: working groups, exercises, shared awareness pilots, decision-rights maps, and concrete industry-academia projects that can be reported back next year.



Session Observations

Why does Houston matter? The opening remarks set a useful tone: maritime risk is not abstract in the Greater Houston-Galveston area. San Jacinto College provided a workforce-focused setting, and the speakers emphasized that the maritime system is both a security environment and an economic engine. The Greater Houston Port Bureau framing was especially important because it linked local port operations to national consequences. The point landed clearly:

Resilience is not only about preventing bad things from happening; it is about keeping commerce, energy flows, emergency response, and community confidence intact when disruptions occur.

Spotlight Speakers: Future-Focused Risk Management

The Coast Guard and Texas Cyber Command keynotes helped establish the symposium as a forward-looking discussion rather than a retrospective review. **Rear Admiral Amy Grable** described a future-development approach that connects foresight, wargaming, research, requirements, and performance analysis to the practical choices organizations make about whether to accept, address, or transfer risk. **Vice Admiral T.J. White**, speaking from the Texas Cyber Command perspective, reinforced that cyber is now a leadership and readiness problem, not a technical niche. Together, the keynotes pushed the audience toward deliberate preparation instead of reactive response.

Cyber threat intelligence: the threat is faster, broader, and less hidden. **Dr. Christopher Porter's** threat briefing gave the cyber discussion urgency. One of the most useful takeaways was that supposedly air-gapped systems often are not air-gapped in practice; informal connections, personal devices, and mismatched diagrams routinely create exposure. The briefing also framed state-backed and criminal activity as a persistent maritime concern, with AI accelerating reconnaissance, exploit development, and data exfiltration. The defensive message was equally practical: know what is connected, maintain a real inventory of devices and



dependencies, isolate what cannot be maintained, and use AI-enabled red teaming and monitoring to close the speed gap.

Day 1 – Panels

USCG Cyber Rules: compliance is now an implementation problem. The regulatory panel made clear that the Coast Guard cyber requirements are moving from awareness to execution. Operators are not all in the same place. Some begin assessments, cybersecurity officer identification, training, and tabletop work early; others are still waiting for guidance. The practical challenge is less about whether cyber matters and more about scope, ownership, and governance. The CISO role, legal exposure, broad IT/OT definitions, workforce scarcity, and the question of "what good looks like" all create friction. The panel's best advice was to start with critical systems, use federal resources, learn from peers, and avoid treating every asset as equally important.

OT/IT Convergence: reliability and security must meet in the middle. The control-systems discussion translated cyber risk into the language of operations. IT values data and connectivity; OT values reliability, safety, and continuity. When those worlds converge, old assumptions break. Legacy PLCs, Windows XP environments, satellite communications, vendor access, USB practices, and flat networks all create openings that may not be fixable with routine patching. The panel repeatedly returned to segmentation, brokered access, read-only defaults, break-glass procedures, critical spares, and tabletop exercises. The most resonant cultural point was that maritime already knows how to build safety habits; cybersecurity needs to become part of that same operational discipline.



AI Guardrails: use AI for better decisions, not novelty. The AI panel avoided hype and focused on consequences. AI can improve visibility, prediction, maintenance, dashboarding, and response speed, but it can also lower the skill barrier for attackers and make false confidence look authoritative. The practical framework was simple: define the decision AI is meant to improve, understand the data it depends on, assign accountability when it is wrong, and maintain a way to operate when AI, data, or systems fail. The strongest guidance was to classify use cases by autonomy and consequence, keep humans in the loop for safety-critical decisions, secure the data pipeline, and build internal AI literacy through hands-on projects.

Risk Assessment: visibility is the first line of defense. The risk panel connected asset discovery to leadership decisions. The discussion compared lightweight scorecards, threat modeling, supplier-risk reviews, and corporate risk matrices that legal, finance, HSE, and operations already understand. That matters because cyber risk only becomes actionable when it is translated into business consequences, prioritization, contracts, and resourcing. The panel also emphasized the value of operators - chief engineers, superintendents, facility security officers, and front line personnel - because they know where the undocumented dependencies and workarounds live. The best assessments were described as multidisciplinary, incident-agnostic, and focused first on the most exposed or business-critical systems.

Operationalizing Cyber Resilience: know the first-hour playbook. The Captain's Watch session closed Day One by turning strategy into execution. The core question was not whether an organization has an incident response plan; it was whether the plan has been exercised enough to work under pressure. The panel emphasized managed alerting, crisis coordination, isolation-and-operate capability, C-suite information requirements, cyber/physical security integration, and realistic drills. A recurring insight was that port disruptions cascade quickly across container operations, inter-modal movement, energy and supply chains, so response cannot be purely technical. Organizations need to know who decides, who calls whom, what gets shared, and how business continuity is maintained while the incident is still unfolding.



Day 2 – Panels

Shipbuilding and Maritime Readiness: risk includes markets, suppliers, and workforce. The Day Two shipbuilding panel broadened maritime risk beyond cyber. The panel described U.S. shipbuilding as a readiness issue shaped by market demand, long-lead suppliers, financing, automation, workforce depth, and acquisition practice. The United States builds quality ships, but delivery timelines, cost, efficiency per ton, and a depleted supplier ecosystem remain major constraints. The conversation repeatedly came back to durable commercial demand as the missing signal that would allow capital, suppliers, and workers to commit. The most actionable opportunities were in advanced manufacturing, robotics, autonomy, alternative fuels, smart ports, workforce development, and commercial acquisition approaches that avoid importing unnecessary military complexity.

Littoral Disruptions: the problem runs from the EEZ to daily life. The littoral disruptions panel captured the biggest systems insight of the symposium: the littorals are where sea, land, rail, pipelines, energy, communications, ports, emergency response, and the defense industrial base converge. The panel discussed dark-fleet tracking, AIS spoofing, metadata analysis, maritime choke points, war-risk insurance, GPS jamming, autonomous sea-denial, and the cost asymmetry of drones and other unmanned systems. The point was not that any single threat dominates. It was that the operating environment is too complex for perfect control, so resilience depends on better dependency mapping, shared awareness, early warning, and exercises that expose second- and third-order consequences.

Maritime Border Security: shared awareness needs trust and vocabulary. The maritime border security discussion placed maritime domain awareness at the center of effective operations. Sensors matter - drones, satellites, radar, cameras, AIS, and real-time information sharing all have a role - but data without analytics, context, and authority is not enough. Speakers emphasized that trust cannot be surged during a crisis, and even common terms such as "dark target" may mean different things to different organizations. The panel also highlighted the



importance of understanding port business operations, legal frameworks, local knowledge, and academic-industry partnerships. The practical requirement is common vocabulary, a shared operating picture, and clear escalation paths before a crisis begins.

Drone and Airspace Awareness: start with detection and integration. The drone/radar technology session made the unmanned systems problem tangible. The discussion covered remote ID, RF sensing, radar, cameras, thermal sensors, AI analytics, middleware, and the need to cue sensors quickly because response time may be measured in seconds or minutes. The legal line was also clear: private entities can generally detect and document drone activity, while mitigation authorities remain constrained. That makes integration with law enforcement and operations centers essential. The Houston Ship Channel scale underscored the challenge: a 52-mile corridor cannot be covered by one organization, and a useful airspace picture will require interoperable systems and multi-partner operating concepts.

Harbor Safety and Security Committees: The SHSU - Institute for Homeland Security (www.ihsonline.org) presented on their partnership with the Port of Brownsville and the role that universities can have in facilitating information sharing. Serving as a broker between federal agencies, the port district, and industry, IHS brought together stakeholders as a catalyst to build trusted relationships. Through relationships, the group developed roadmap for creating bi-laws establishing the Rio Grande Valley Waterways Advisory Committee (RGVWAC). The discussion with representatives from the Port of Brownsville, Sector Corpus Christi, G and H Towing, SHSU/IHS highlighted the value of charters, recurring collaboration, local expertise, and practical information sharing. These committees are not glamorous, but they are exactly where resilience gets operationalized. They give port authorities, industry, operators, and government partners a standing venue to improve safety, security, mobility, environmental protection, situational awareness, and rapid response.



Closing Discussion

MRS2027 should report progress. The closing conversation and Symposium Sense inputs pointed toward a more action-oriented MRS2027. Participants asked for a tabletop or wargame that shows both normal operations and what wrong looks like under catastrophe; a roster or trust network to support collaboration; deeper industry participation; human-machine teaming; better information sharing; and a demonstration of IT/OT integration failure modes. Suggested working groups included drone/counter-drone, cross-organization coordination and a single-pane-of-glass awareness concept, AI and maritime risk, and "paying it forward" through education and workforce development. The appetite was clear: keep the community connected and bring evidence of progress next year.

Overall Event Readout

The event felt well-aligned to the moment. MRS2026 had a clear through-line from opening remarks to closing discussion. The agenda began with cyber and AI because those are immediate pressure points for ports, vessels, energy companies, and regulators. It then widened into the physical, industrial, and governance dimensions of maritime risk. That sequencing worked. It allowed Day One to build a common operating picture around digital risk, then used Day Two to remind the audience that cyber is only one way a maritime system can be disrupted.

The Houston location sharpened the discussion. Because the symposium took place in the Houston-Galveston ecosystem, speakers were able to keep returning to real stakes: energy flows, petrochemical production, workforce pipelines, cruise and cargo operations, ship channel dependencies, and the practical burden on local responders and operators. That gave the sessions a grounded feel. The conversations did not drift into generic resilience language; they stayed connected to ports, waterway committees, terminals, vessels, shipyards, operations centers, and the people who have to keep the system running. The mix of participants was a strength. The event brought together regulators, Coast Guard leaders, port and industry representatives, cyber practitioners, technology vendors, academics,



students, and infrastructure partners. That mix mattered because no single sector can see or manage the whole risk picture. The best moments came when panels crossed boundaries: cyber experts speaking with facility security and operations leaders, maritime domain awareness discussions tied to data governance and trust, shipbuilding linked to workforce and capital markets, and drone detection framed as an operating concept rather than a gadget discussion.

The practical examples carried the most weight. The sessions were strongest when speakers moved from principle to lived experience: air-gaps that are not really air-gapped, tabletop exercises that expose gaps, port disruption cascading into intermodal congestion, AIS and dark-fleet ambiguity, CISO role confusion, legacy OT that cannot simply be patched, drone detection across a long ship channel, and harbor safety committees that turn relationships into standing practice. Those examples made the event feel useful to operators as well as policy audiences.

The main improvement opportunity is follow-through. The symposium generated a lot of energy and a broad set of ideas. The next step is to convert that energy into named owners, working groups, exercises, and measurable outputs. The QR/app collection process was a good start because it captured audience insight that would otherwise disappear after the event. The most valuable MRS2027 would not simply repeat the same risk themes; it would show what the community did with them during the year.



Cross-Cutting Takeaways

1. Maritime risk is now a cross-sector cascade problem, not a maritime-only problem. A disruption in the littorals can quickly spill across ports, shipping, trucking, rail, pipelines, energy, telecom, insurance, manufacturing, military readiness, emergency management, and local communities. The strongest planning need is not another list of hazards; it is a shared dependency map that shows second- and third-order effects. MRS2027 should use a tabletop or wargame to make those cascades visible to senior leaders.
2. Cyber resilience must move from compliance and plans to operational muscle memory. The Coast Guard rules, MTSA plans, CISOs, asset inventories, and training requirements all matter, but paperwork will not hold up unless it is tied to practice. Organizations need exercised decision rights, first-hour communications, isolation-and-operate procedures, critical spares, vendor contacts, and business-continuity playbooks. The practical test is simple: can the organization keep operating, safely and lawfully, while the cyber event is still confusing?
3. AI is both a threat accelerator and a defensive force multiplier. AI showed up in almost every lane: threat intelligence, exploit generation, OT targeting, digital twins, predictive maintenance, dashboards, workforce development, and education. The mature posture is not "use AI everywhere." It is to use AI where it improves speed, visibility, and judgment; protect the data pipeline; classify use cases by consequence; keep humans in the loop for safety-critical actions; and maintain a failure playbook when the model, data, or connected system is unavailable. [Sam Houston State University | Huntsville, TX 77341 | www.ihsonline.org](https://www.ihsonline.org)



4. Shared awareness requires interoperability, trust, and decision authority - not just more sensors. Maritime data exists everywhere, but it does not automatically create understanding. AIS can be spoofed, radar and cameras can be siloed, drone alerts can lack context, and organizations may use different words for the same event. The community needs common vocabulary, shared escalation guides, interoperable systems, data-sharing rules, and living decision-rights maps that clarify who can act, who must be informed, and what happens next.
5. Maritime readiness is a market, workforce, and supply-chain challenge as much as a security challenge. The shipbuilding discussion made clear that maritime strength depends on durable demand signals, investable markets, supplier confidence, workforce depth, port infrastructure, automation, and acquisition choices. Cyber and physical security should be built into new systems from the start, but the bigger readiness challenge is sustaining the industrial base and talent pipeline that allow the country to build, maintain, secure, and surge maritime capability.
6. Partnerships need a year-round operating model. The best relationships at MRS were not ceremonial; they were functional. Area maritime security committees, harbor safety committees, ISACs, port bureaus, universities, national labs, vendors, and operational agencies all have pieces of the solution. The next step is to assign work between conferences: name working groups, set measurable outputs, capture participant networks, run exercises, and bring results back to MRS2027.



Suggested Next-Year Work Products

- a. **Exercise Package:** A cross-sector tabletop or wargame that begins in normal operations, introduces cyber/physical/autonomous disruptions, and forces decision-making under incomplete information.
- b. **Decision-Rights Map:** A practical guide for who calls whom, who decides, what gets shared, and how authorities change across cyber, drone, port security, and emergency management scenarios.
- c. **Shared-Awareness Pilot:** A small, operationally realistic demonstration that fuses port, vessel, drone, cyber, and infrastructure signals into a usable picture for multiple partners.
- d. **Working Groups:** Drone/counter-drone, AI and maritime risk, cross-organization coordination, port partnership models, and maritime workforce/industrial-base readiness.
- e. **Source materials reviewed:** final MRS2026 agenda, Day One and Day Two Panel Videos, prepared session summaries, Symposium Sense/QR inputs, and the MRS website.

Appendix A: One Drive Links to Conference Materials

Day 1 & Day 2 Slide Decks:

https://myshsu-my.sharepoint.com/:f:/g/personal/slp082_shsu_edu/lgA4WKwnAkziQI5fUdUkr6LFAbXFtjs-n5MinjlobXQl-Yw?e=1ZpF7k

Research Papers:

https://myshsu-my.sharepoint.com/:f:/g/personal/slp082_shsu_edu/lgBtfjkpQsXeQ74VKz9xX4JRATxWhE03NCl2VKZeTWtCnTQ?e=Gw7krF

Website: <https://www.maritimerisksymposium.org/>

Conference Photos:

https://myshsu-my.sharepoint.com/:f:/g/personal/slp082_shsu_edu/lgAuwaUYTMNsQ5UPcHD8paEVATJNjJBoYPH_ObjkATOXS6I?e=H6v0gG

Appendix B: Unlisted YouTube Links for All Sessions

Keynote Speakers

<https://youtu.be/JbtB3Gax7Ck>

Panel 2: Navigating the New Normal: USCG Cyber Rules & Industrial Reality

<https://youtu.be/tMa577mWUck>

Panel 3: Securing the Converged OT/IT Environment

https://youtu.be/BbmnK_u6yoE

Panel 4: Guardians of the Guardrails: Securing Artificial Intelligence in Maritime Operations

<https://youtu.be/vtp9Q0LqwKk>

Panel 5: Charing the Unknown: From Asset Discovery to Strategic Resilience

https://youtu.be/cQOnq_kKozM

Panel 6: Putting it All Together: The Captain's Watch, Operationalizing Cyber Resilience

<https://youtu.be/cwW54Av7vTw>

Panel 7: Forging Maritime Readiness through U.S. Shipbuilding, Supply Chains, and Workforce

<https://youtu.be/4GIHwAVEmzU>

Panel 8: Littoral Disruptions & Cascading Consequences on Private Industry

https://youtu.be/Xyt6Z_rlyGw

Panel 9: Maritime Border Security

<https://youtu.be/kshJSfal1oE>

Panel 10: Addressing Elements of Maritime Risk from the Sky

<https://youtu.be/qS-0NmHBNoO>

Panel 11: Harbor Safety & Security Committees: A Case Study

<https://youtu.be/QIkLkrjXwzM>



www.maritimerisksymposium.org
www.ihsonline.org



Sam Houston
State University
MEMBER THE TEXAS STATE UNIVERSITY SYSTEM