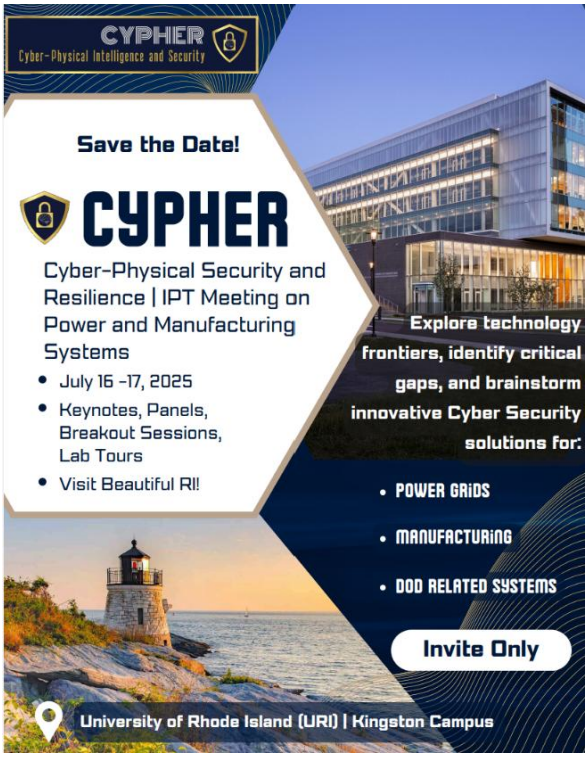
CYPHER IPT Meetings 2025

Event Report

July 16–17, 2025 | University of Rhode Island



Executive Summary

The 2025 CYPHER IPT Meetings (July 16–17, University of Rhode Island) convened leaders from government, industry, and academia for two days of focused collaboration on cyber-physical system security and resilience across power systems, advanced manufacturing, and naval applications. The program combined keynote and panel discussions with student-led demonstrations, lab tours, and structured breakout dialogues to accelerate alignment between research priorities and operational needs.

Why this matters: The IPT accelerates movement from promising ideas to **field-relevant prototypes** by aligning researchers, operators, and industry around shared needs and transition paths to Navy programs.

A key outcome of the meeting was strengthened cross-sector partnership development and clear momentum toward follow-on collaboration. Discussions identified shared technical priorities—including secure modernization of legacy operational technology, resilient energy and manufacturing ecosystems, and the trustworthy application of AI and digital twins in mission-critical environments—while emphasizing the importance of closing the gap between early-stage research and deployable solutions. The event also catalyzed emerging collaborations, including planning for cross-site cyber-physical testbed integration and new student-focused engagement pathways that connect workforce development with sponsor and partner priorities.

Naval relevance was reinforced through an invitation-only, CUI-level IPT session dedicated to naval applications, enabling deeper technical exchange aligned with the Department of War's needs. This closed session supported candid discussion of cyber-physical challenges in shipboard systems and shipbuilding/maintenance environments, and helped identify pathways for continued government–industry–academia coordination under appropriate information controls. URI and Rite-Solutions are uniquely positioned to **convene Navy stakeholders with industry and academia**, create a **trusted CUI-capable forum**, and fund the early work needed to de-risk technologies before they transition to acquisition and fleet adoption.

Looking ahead to 2026, participants and organizers recommended expanding to a two-day open meeting followed by a full-day CUI session, sharpening annual objectives and deliverables, and improving mechanisms for capturing outcomes (e.g., structured note capture and actionable reporting). Additional priorities include broadening mission-focused participation, refining panel formats to maximize discussion, and increasing structured opportunities for collaboration, student engagement, and targeted breakout work.

Outcomes at a Glance

• Partnership momentum: Cross-sector connections strengthened and follow-on collaborations initiated (including testbed and workforce pathways).

• Naval relevance advanced: CUI session enabled deeper problem framing and solution pathway discussions aligned to Navy needs under appropriate controls.

• 2026 actions: Recommended 2-day open IPT + full-day CUI session, clearer objectives/deliverables, and improved capture of actionable outcomes.

• Acceleration mechanisms: Student demos, focused breakouts, and partner read-aheads to speed down-selects toward pilots and demonstrations.

• URI and Rite-Solutions unique role: Convene the right stakeholders, enable trusted CUI-capable collaboration, and fund early de-risking that supports transition to the Fleet.

Event Overview

The 2025 CYPHER IPT Meetings held July 16–17 at the University of Rhode Island, brought together leaders from academia, industry, and government for two days of focused collaboration on Cyber-Physical System Security and Resilience in power systems, manufacturing systems, and naval applications.

Day 1 featured keynote talks, expert panels, student-led demonstrations, lab tours, and breakout sessions that examined critical challenges in power and energy systems and advanced manufacturing.

Day 2 began with interactive dialogues among industry, academic, and government leaders, followed by an invitation-only, CUI-level workshop that enabled in-depth discussions and partnership-building aligned with Department of Navy priorities.

The meetings produced partner-matched follow-on actions (testbed integration, student workforce pathways) and will inform the 2026 event format, reinforcing a clear throughline from research to fleet-relevant solutions.

Acknowledgments

We thank Dr. Marc Parlange (President, URI), Dr. Bethany Jenkins (Vice President for Research), and Amy Carroll (Associate VP for Research Initiatives and Development) for their inspiring video and in-person welcome remarks, which set an energizing tone from the very start. We are also grateful to Dr. Anthony Marchese (Dean, College of Engineering) for his support in inviting our keynote speaker and sponsoring the event catering.

We extend our appreciation to Dr. Michele Anderson (Program Officer, ONR Code 332) for her participation on the IPT organizing committee and her ongoing support of collaborative

research efforts aligned with Naval priorities. Our core organizing team—Dr. Yan (Lindsay) Sun, Dr. Manbir Sodhi, Dr. Tim Arcano, Mr. Paul Boivin, Dr. Hui Lin, Dr. Kaushallya Adhikari, and Ms. Chelsie Sullivan—played an indispensable role in planning, coordination, and on-site execution.

We thank Mr. Ray Gabriel (Vice President of Strategic Operations, General Dynamics Electric Boat) for his keynote remarks highlighting the urgency of securing energy systems, manufacturing, and shipbuilding in support of U.S. maritime defense capabilities.

We thank our panelists:

Panel 1: Power System Resilience and Security, moderated by Dr. Yan (Lindsay) Sun, featuring Greg Belanger, Chief Technology Security Officer, PPL Corporation; Dr. Esther Amullen, Program Lead for Cybersecurity Data & Analytics, EPRI; Dayne Broderson, Senior Technologist & Strategic Advisor, Alaska Center for Energy & Power; LCDR Jennifer Rogers, Cyber Systems Program Chair, U.S. Coast Guard Academy; and Dr. Hui Lin, CYPHER Tech Director, URI.

Panel 2: CPS Challenges in Industry 4.0 Shipbuilding, Maintenance & Repair, moderated by Dr. Tim Arcano, including Daniel Reed, Executive Director, Naval Shipbuilding & Advanced Manufacturing COE; William Barnes, Chief Information Security Officer, General Dynamics Electric Boat; Frank Krazer, Systems Engineer, Manufacturing Intelligence Division, Hexagon; and Dr. Manbir Sodhi, CYPHER Co-Director, URI.

Finally, we extend our heartfelt appreciation to **all attendees** for bringing their expertise and innovative thinking to fulfill the mission of the IPT meeting as one collaborative team. Special recognition goes to our student participants for delivering exceptional demos and posters and for managing every logistical detail.

We eagerly anticipate reuniting in Rhode Island in Summer 2026 for an even more enriching experience alongside an expanded network of peers.

Organizing Committee:

Dr. Yan (Lindsay) Sun	*Professor, CYPHER Center Co-Director, URI*
Dr. Manbir Sodhi	*Professor, CYPHER Center Co-Director, URI*
Dr. Tim Arcano	*Chief Technology Officer, Rite-Solutions, Inc.*
Mr. Paul Boivin	*Senior Cybersecurity Engineer, Rite-Solutions, Inc.*

Dr. Hui Lin	*Associate Professors, URI, Demo and Poster Session*
Dr. Kaushallya Adhikari	*Co-Chairs*
Ms. Chelsie Sullivan	*CYPHER Center Coordinator, Local Arrangement Chair*
Dr. Michele Anderson	*Program Officer, Office of Naval Research*

CYPHER IPT Open Meeting | Agenda

Meeting Title: Cyber-Physical Security and Resilience (CYPHER) Integrated Project Team Meeting on Power and Manufacturing Systems
Purpose: Align partners on high-impact challenge areas and define follow-on actions that move promising approaches toward demonstration and transition.

July 16 | Day 1

TIME	DESCRIPTION	LOCATION
8:00 am	Arrival, Registration & Breakfast	FCAE 025
9:00 am	Welcome Remarks	FCAE 025
9:20 am	Keynote Address with Ray Gabriel, Vice President, Strategic Operations, General Dynamics Electric Boat	FCAE 025
10:00 am	Panel on Power System Resilience and Security	FCAE 025
11:05 am	10-min Break	
11:15 am	Panel on Shipyard 4.0	FCAE 025
12:30 pm	Lunch, Interactive Demos and Lab Tours	FCAE 465, 180A
2:30 pm	Breakout Discussion Sessions	FCAE 025, 010, 040
4:00 pm	10-min Break	
4:10 pm	Breakout Session Summary Reports	FCAE 025
5:00 pm	Adjourn	FCAE 025

July 17 | Day 2 Morning

TIME	DESCRIPTION	LOCATION
8:30 am	Interdisciplinary Breakfast Dialogues	FCAE 025

10:00 am	Reflections and future directions with Industry, Academia, and Government leaders	FCAE 025
11:30 am	Closing Remarks and Adjourn	FCAE 025

CYPHER IPT CUI Meeting | Agenda

Meeting Title: Cyber-Physical Security and Resilience (CYPHER) CUI Integrated Project Team (IPT) Meeting for Naval Applications
Purpose: Enable candid, operationally grounded discussion of naval cyber-physical risk and solution pathways under appropriate information controls.

July 17 | Day 2 Afternoon

TIME	DESCRIPTION	LOCATION
11:45 pm	Arrival, Registration & Lunch	Galanti Lounge
12:00 pm	**Lunchtime Presentation:** Maritime Network Fingerprinting on NMEA2000 Protocol	Galanti Lounge
12:30 pm	**Naval Application Keynote Address** with Ken Fischer, Chief of Cybersecurity, SSTM, NSWC Philadelphia Division	Galanti Lounge
1:00 pm	**Panel 1:** CPS Security and Resiliency Challenges in Shipboard Systems	Galanti Lounge
2:05 pm	10-min Break	
2:15 pm	**Panel 2**: CPS Challenges in Industry 4.0 Shipbuilding, Maintenance, and Repair	Galanti Lounge
3:30 pm	Closing Remarks	Galanti Lounge
4:00 pm	Adjourn	Galanti Lounge

Speaker Bios | Open Sessions

Keynote Speaker

Ray Gabriel

Vice President, Strategic Operations, General Dynamics Electric Boat

Ray Gabriel leads strategic operations for General Dynamics Electric Boat, bringing an industry perspective on scaling secure, resilient shipbuilding and industrial operations that directly support fleet readiness and modernization.

Panel 1: Power System Resilience and Security

Moderator: Dr. Yan (Lindsay) Sun

University of Rhode Island Professor, ECBE Department Chair, CYPHER Co-Director

Panelist 1: Greg Belanger

Chief Technology Security Officer, PPL Corporation

Greg Belanger is Chief Technology Security Officer at PPL Corporation, focused on modernizing cybersecurity for large-scale critical infrastructure and advancing practical approaches to protect operational technology that parallels Navy industrial and energy challenges.

Panelist 2: Dr. Esther Amullen

Principal Technical Leader in Cybersecurity, EPRI

Dr. Esther Amullen is a cybersecurity and AI leader at EPRI, advancing data-driven security methods for electric power and operational technology environments—insights that help translate research into deployable practices for mission-critical systems.

Panelist 3: Dayne Broderson

Computer and Information Research Scientist, Alaska Center for Energy and Power (ACEP)

Dayne Broderson supports cyber capacity and resilient energy efforts at the Alaska Center for Energy and Power (ACEP), connecting testbeds, applied research, and partner needs to accelerate real-world demonstrations and workforce development.

Panelist 4: Dr. Jennifer Rogers

Cyber Systems Program Chair, US Coast Guard Academy

LCDR Jennifer Rogers leads cyber systems education at the U.S. Coast Guard Academy and contributes operationally grounded expertise on securing critical systems—bridging workforce development, mission needs, and applied research.

Panelist 5: Dr. Hui Lin

Associate Professor, University of Rhode Island, CYPHER Technical Director

Dr. Hui Lin is CYPHER's Technical Director at URI, leading research and testbed-driven work in cyber-physical security for power and manufacturing systems, with an emphasis on methods that can be evaluated in realistic operational environments.

Panel 2: Shipyard 4.0

Moderator: Dr. Tim Arcano, Rite-Solutions

Panelist 1: Daniel Reed

Executive Director, Naval Shipbuilding and Advanced Manufacturing Center of Excellence, ATI

Daniel Reed leads the Navy ManTech Naval Shipbuilding and Advanced Manufacturing Center of Excellence, bringing direct experience in shipyard modernization and technology transition pathways that inform fleet-relevant manufacturing priorities.

Panelist 2: William Barnes

Chief Information Security Officer, General Dynamics Electric Boat

William Barnes is CISO at General Dynamics Electric Boat, leading cybersecurity strategy and operations for a major naval shipbuilder and providing perspective on risk reduction and implementation at enterprise scale.

Panelist 3: Frank Krazer

Systems Engineer, Hexagon Metrology

Frank Krazer is a systems engineer at Hexagon Manufacturing Intelligence, focused on integrating measurement and industrial automation—relevant to secure Industry 4.0 adoption and resilient shipyard/manufacturing workflows.

Panelist 4: Dr. Manbir Sodhi

Professor, University of Rhode Island, CYPHER Co-Director

Dr. Manbir Sodhi is a CYPHER Co-Director at URI, specializing in advanced manufacturing systems and optimization, and helping shape IPT discussions toward practical demonstrations and transition-ready outcomes.

Speaker Bios | CUI Session

Keynote Speaker

Dr. Ken Fischer
Chief of Cybersecurity (SSTM), NSWC Philadelphia Division

Keynote Address: Firewalls Can't Stop Flooding: Reframing Cybersecurity for Shipboard Control and Cyber-Physical Systems

Dr. Ken Fischer is Chief of Cybersecurity (SSTM) at NSWC Philadelphia Division, leading HM&E cybersecurity efforts and framing shipboard cyber-physical risk in ways that drive actionable R&D priorities for naval platforms.

CUI Panel 1: CPS Security and Resiliency Challenges in Shipboard Systems

Moderator: Mr. Paul Boivin
Senior Cybersecurity Engineer, Rite-Solutions, Inc.

Panelist 1: Dr. Ken Fischer
Chief of Cybersecurity (SSTM), NSWCPD [Bio Above]

Panelist 2: Mr. Steve Masterson
Director, Cybersecurity Undersea Warfare (SSTM), NUWCDIVNP

Steve Masterson directs Cybersecurity Undersea Warfare at NUWC Newport, bringing fleet-facing systems engineering and cybersecurity leadership that helps prioritize practical solutions for undersea warfare and shipboard systems.

Panelist 3: Dr. Ben Drozdenko
Cybersecurity S&T Lead, NUWCDIVNPT

Dr. Ben Drozdenko is the Cybersecurity S&T Lead at NUWC Newport, guiding R&D in AI/ML-enabled cyber situational awareness and survivability and connecting emerging approaches to Navy mission needs and transition opportunities.

Panelist 4: Mr. Joe Bransfield
Fleet Cyber Liaison, NUWCDIVNPT

Joe Bransfield is NUWC Newport's Fleet Cyber Liaison, translating operational realities into technical priorities and supporting cyber readiness through exercises, testing, and on-platform evaluation—ideal for shaping actionable IPT outcomes.

CUI Panel 2: CPS Challenges in Industry 4.0 Shipbuilding, Maintenance, and Repair

Moderator: Dr. Tim Arcano
Chief Technology Officer, Rite-Solutions, Inc.

Panelist 1: Daniel Reed
Executive Director, Naval Shipbuilding and Advanced Manufacturing Center of Excellence, ATI

[Bio Above]

Panelist 2: Michael Chung
CTO, Maritime Technology Group

Michael Chung is CTO at Maritime Technology Group with experience modernizing cybersecurity across public and private sectors; he contributes a transition-focused view of how to move innovations into operational practice.

Panelist 3: Dr. Manbir Sodhi
Professor, University of Rhode Island, CYPHER Co-Director

[Bio Above]

Panelist 4: Wayne Austad
CTO, National & Homeland Security Directorate; Idaho National Laboratory

Wayne Austad is CTO for National & Homeland Security at Idaho National Laboratory, leading partnerships and applied R&D in secure and resilient cyber-physical systems that align with Navy-relevant infrastructure and industrial challenges.

Panelist 5: Benjamin Lampe
Cybersecurity Researcher; Idaho National Laboratory

Benjamin Lampe is a cybersecurity researcher at Idaho National Laboratory focused on cyber-informed engineering and practical resiliency methods for operational technology—relevant to improving system robustness in mission-critical environments.

Live Demonstrations and Posters

One of the most impactful components of the 2025 CYPHER IPT Meetings was the series of live demonstrations delivered by students and researchers across both days. These interactive sessions showcased cutting-edge work in cybersecurity, power systems, and

manufacturing, offering attendees a hands-on look at emerging technologies and applications. As noted in the Feedback & Next-Year Vision Summary, participants strongly supported expanding demo time and introducing structured formats like lightning talks to enhance engagement and visibility. These recommendations will guide future planning as the event continues to serve as a platform for collaboration and technical exchange.

Live Demonstrations List:

These demonstrations provide a rapid way to test ideas early, get feedback from operational and industry experts, and identify which approaches are most promising for near-term pilot efforts.

No.	Title	Location
1	When Agentic AI meets Digital Twin – Cyber-physical response to grid anomalies	FCAE 465
2	Large Language Model on Edge Neural Processing Unit (NPU): Ultra-low Power, Fast Inference AI with Ultimate Privacy	FCAE 465
3	Encrypted Design Blocking: A Network-Level Defense Evasion	FCAE 465
4	Multi-Agent LLM Assistant for Power System Digital Twin	FCAE 465
5	CYPHER Cell SMART Manufacturing Testbed	FCAE 180A
6	Secure CNC Fingerprinting	FCAE 180A
7	ASRS Autoloader Cell	FCAE 180A
8	Hexagon Scanning Arm	FCAE 180A

Report 1: Breakout Session Report – Power and Energy Systems

Part 1: The group discussion highlights several critical and interconnected themes.

Key Takeaways (Non-Technical):

- **Main challenge:** Many critical systems were not designed with cybersecurity in mind, so upgrades must be practical and phased.
- **Main risk:** Technology is changing faster than policy, training, and implementation.
- **Main blocker:** Workforce gaps—especially "operators who understand both operations and cybersecurity."
- **What success looks like:** Test solutions in realistic environments, prove value quickly, and scale what works.
- **Next step:** Use shared testbeds and partner pilots to move from concepts to transition-ready demonstrations.

Technical Detail (for interested readers)

1. **The "Legacy vs. Modernity" Conundrum:** This is the central tension. How do you implement cutting-edge security (Zero Trust, AI) and leverage new technologies (Digital Twins, Cloud) when the foundational infrastructure (OT systems) wasn't built with security in mind and has an incredibly long lifecycle? This isn't just a technical problem, but also economic and regulatory.
2. **The Human Element as Both Problem and Solution:**
    - **Workforce Crisis:** The aging workforce and the lack of specific OT/ICS cybersecurity skills is a massive vulnerability.
    - **AI Literacy Gap:** A significant barrier to adopting advanced tools, from executives making decisions to personnel using them.
    - **Cultural Resistance:** To AI, to change, to new security paradigms, often stemming from valid data concerns or simply inertia.
    - **Training & Education:** A clear path forward, exemplified by your GenAI training initiatives.
3. **The Accelerating Pace of Change vs. Slow Adoption/Regulation:** Technology is moving at warp speed (AI, distributed energy, new attack vectors), while policy, regulation, and organizational adoption cycles are much slower. This creates a widening gap of vulnerability. **The Attack Surface is Expanding from Emerging Technologies.** While offering opportunities, technologies like renewable energy

(distributed systems), Digital Twins, and AI agents inherently increase complexity and potential entry points for adversaries.

4. **The ROI & Policy-Proofing Challenge:** How do you justify significant cybersecurity investments when the returns aren't always immediately visible, and policies/regulations shift frequently, potentially "pulling the rug out" from under long-term strategies? This is particularly acute for critical infrastructure where the costs should not be passed on to consumers.
5. **Bridging the Research-to-Practice Gap:** There's a clear desire to move academic innovation (TRL 1-3) closer to real-world industrial impact (TRL 4-8), emphasizing community-partnered testbeds and "boots on the ground" collaboration.

Part 2: Summary of Challenges and Solutions

Key Challenges:

- **Legacy OT Systems:** Inherently insecure by design, extremely costly and complex to replace/upgrade, not built for modern threats or security paradigms.
- **Retrofitting Zero Trust:** Significant architectural, technical, and operational hurdles to apply Zero Trust principles to existing, often proprietary and isolated, OT environments.
- **Rapid Technological Pace:** The accelerated speed of innovation (AI, Digital Twins, distributed energy) far outpaces organizational adoption, regulatory frameworks, and policy updates.
- **Expanding Attack Surface:** Increased complexity from distributed renewable energy, multi-actor systems, and emerging technologies (AI agents, Digital Twins) creates more entry points for adversaries.
- **Critical Workforce Gaps:** An aging OT workforce, severe shortage of specialized OT/ICS cybersecurity talent, and a widespread lack of AI literacy across all organizational levels.
- **AI Adoption Barriers:** Pervasive concerns over data privacy (especially for sensitive OT data in cloud-based AI), inaccurate assumptions about AI capabilities, and organizational resistance to new tools.
- **Policy & Regulatory Lag:** Energy policies and regulations (both national and international) are slow to adapt to evolving threats and technological shifts, creating instability for long-term investments.
- **ROI & Economic Justification:** Difficulty in demonstrating clear return on investment for cybersecurity expenditures.

- **Complexity of Emerging Tech:** Ambiguity in definitions (e.g., Digital Twins), architectural challenges, and new attack vectors associated with AI algorithms and Digital Twin data integrity.
- **Research-to-Practice Gap:** A significant gap between cutting-edge academic research (TRL 1-3) and the practical, immediate needs and maturity levels (TRL 4-8) of industrial operators.
- **Data Governance & Quality:** Challenges in ensuring data quality and appropriate governance for security data lakes feeding business intelligence and AI applications.
- **Physical & Latency Constraints:** Strict physical tolerances and latency requirements in OT systems hinder the implementation of virtualization, monitoring, and other security overlays.

Proposed/Implied Solutions:

- **Strategic Legacy System Evolution:**
    - Implement "bump in the wire" solutions (e.g., secure gateways, edge proxies, virtualization) to augment existing systems rather than full replacement.
    - Utilize digital twins of legacy systems to facilitate safer testing, gradual evolution, and understanding of their behavior.
- **Targeted Architecture Improvements for Cyber-Resiliency:**
    - Focus on appropriate architectural designs that can accommodate the unique constraints and requirements of OT domains when considering Cyber-Resiliency tenets.
- **Comprehensive Workforce Development:**
    - Foster Interdisciplinary Talent: Enhance workforce capabilities through tailored training programs that integrate best practices and strengthen collaboration between industry and academia.
    - Cultivate Responsible Innovation: Promote a cultural shift by providing secure environments for the safe exploration and adoption of emergent technologies, leveraging AI as a powerful tool.
    - Prioritize Human-Centric AI: Ensure effective and ethical technology integration by emphasizing human-in-the-loop approaches in all AI applications.
- **Bridging Research & Industry:**
    - Establish community-partnered testbeds to ground academic research in real-world problems and accelerate practical impact.

    - Encourage local ownership of cyber risk and foster ground-up, industry-driven solutions.
    - Shift academic focus towards solutions with immediate impact at industry maturity levels (e.g., TRL 4-8).
    - Facilitate greater collaboration and communication between academics and "boots on the ground" practitioners.
- **Prudent & Secure Emerging Tech Adoption:**
    - Develop and explore in-house LLMs to address concerns about sending sensitive OT data to cloud-based AI.
    - Invest in robust risk assessment methodologies specifically designed for rapidly evolving AI and Digital Twin environments.
    - Define and implement appropriate architectures for Digital Twins to manage their inherent complexity and expanded attack surface.
- **Proactive Policy & Regulatory Engagement:**
    - Actively engage with regulators to educate them on technological advancements and advocate for policies that keep pace with threats and support necessary investments.
    - Develop strong business cases for essential upgrades, highlighting long-term ROI and risk mitigation to regulators.
- **Focus on Lifecycle Management & Value:**
    - Adopt a lifecycle model for technology investments, acknowledging the long operational lifespans of OT systems.
    - Communicate the long-term value proposition of cybersecurity in terms of resilience, operational stability, and risk avoidance.
- **Enhanced Collaboration & Communication:**
    - Foster continuous communication and partnerships across academia, industry, and government entities (e.g., CISA).
    - Promote the sharing of collective wisdom and best practices within the OT cybersecurity community.

Breakout Session Summary – Manufacturing

The Manufacturing breakout session identified several priority areas: the need to address cyber threats in manufacturing and proactively manage IIoT risks for both industry and defense; the importance of summarizing supply chain vulnerabilities and broader systemic threats; and the potential of advanced modeling using integrated toolsets. Participants recommended increasing shipbuilding and manufacturing technology demonstrations and discussions, improving panel formats with quicker introductions and no slides for panelists, and expanding the number of demos in future events. The session also confirmed the development of an Industry 4.0 course in collaboration with Hexagon.

Report 2: Breakfast Discussion Report – Feedback and Next Year Vision

Participants and organizers offered thoughtful and constructive feedback on the 2025 CYPHER IPT Meetings. These recommended changes are designed to make the 2026 IPT more outcome-driven—**faster alignment, clearer decisions, and more direct pathways to demonstration and transition.**

Event Structure & Strategic Vision

- Use “CYPHER IPT Meetings” branding to reflect a defined identity
- Expand format to a two-day Open IPT meeting followed by a one-day CUI IPT session.
- Maintain an invitation-only format, with a cap on attendance based on URI’s venue capacity.
- Introduce a nomination system for current participants to recommend future attendees based on interest areas and expertise.
- Add on-site student recruitment and career advising, including demos/posters for student engagement.
- Reserve small conference rooms to support focused, deep-dive collaboration.

Student Engagement & Visibility

- Extend time for student demos to encourage meaningful conversations
- Add lightning talks or 60-second elevator pitches so attendees can identify projects of interest.
- Embed students in breakout groups to build confidence and develop professional networking skills.
- Explore URI–Alaska student exchange projects and AUSI integration for summer 2026.

Program Format & Depth

- Introduce micro-courses or workshops as breakout options for in-depth learning.
- Offer multiple session tracks (e.g., cyber, manufacturing, digital twins) tailored to different participant interests.
- Provide a thematic focus for the meeting to guide submissions, breakout group formation, and presentations.

Panels & Keynotes

- Keep panel introductions brief and eliminate slides; transition quickly into meaningful discussion.
- Distribute presenter and attendee bios in advance to improve engagement and preparation.
- Invite a more technical keynote speaker on Day 1 to frame the technical depth of the event.
- Preserve and expand the CUI keynote and session, which received strong positive feedback.

Collaboration Tools & Technology Integration

- Use audio recording and automatic transcript generation to capture breakout discussions.
- Require designated PoCs to submit summaries using tools like ChatGPT/NIPRGPT for report generation.
- Ensure reliable internet access across venues to support collaboration tools.
- Assign a representative ("voluntold") to report out for each breakout group to ensure clear and consistent documentation.

Future Collaborator Inclusion

- Invite new stakeholders such as Naval Reactors (NR/08), NSWC Philadelphia, and ADM Caldwell's operational command.
- Build panels or breakouts around Operational Technology (OT) topics, including zero-trust, HM&E systems, and shore-based platforms.
- Encourage industry to present statements of need, while offering academia unsolved, high-value challenges.

CUI & Security Protocols

- Expand the CUI session to a full day for more in-depth technical collaboration.
- Clarify clearance processes (e.g., DISS usage for visit authorization) well in advance.
- Reinforce protocols for handling Controlled Technical Information (CTI) and Distribution D discussions.

Logistics & Participation

- Event logistics, including name tags and food, were well received and should be maintained.

- Emphasize referral mechanism for attendees to recommend colleagues aligned with the event's focus.
- Use submitted bios and themes to curate attendee lists, breakout groups, and collaboration matches.

Report 3: Outcome of Networking & Collaboration

Ample time for informal discussions, lab tours, working meals, and breakout sessions enabled participants to identify shared challenges, align research interests, and spark new collaborations.

- **Joint Research Development**
  Shared interests include digital twins, resilient energy systems, cyber-physical security, and on-premise LLMs. These efforts align with ONR priorities and ongoing A3/A4 grant activities.
- **Cyber-Physical Testbed Integration**
  URI's OPAL-RT system and ACEP's CAMIO/Design Lab will be integrated to co-develop a cross-site sandbox environment for experimentation and learning.
- **Student Collaboration & Exchange**
  Plans are underway to engage URI and UAF students in joint technical projects, including potential summer internships in Alaska and AUSI project co-development for 2026.
- **Strategic Planning for CYPHER IPT 2026**
  ACEP will co-lead event planning, emphasizing high-impact demonstrations and expanded participation from federal and industry partners.
- **Coast Guard Collaboration Opportunities**
  Initial discussions with U.S. Coast Guard representatives explored joint research on Alaska-relevant cyber and marine energy challenges, with follow-up activities planned.

The CYPHER IPT presents unique value to the Navy by enabling these partnerships to move quickly, linking Navy needs and trusted collaboration venues to accelerate feasibility demonstrations and de-risk transition to fleet applications.

Photos from the Event

Photo 1 - Dr. Yan (Lindsay) Sun moderates Panel 1, introducing panelists and setting the stage for discussion on Day 1.

Photo 2- co-organizers Dr. Manbir Sodhi (in person) and Dr. Tim Arcano (joining remotely) respond to audience questions during a dynamic Q & A session

Photo 3- URI postdoctoral researcher Romesh Prasad delivers a live demonstration in the Manufacturing Lab, showcasing applied innovation on Day 1

Photo 4- URI Ph.D. student Anissa Elias presents her research in the CYPHER Lab to an engaged audience

Photo 5, 6 and 7- Academic, government, and industry participants collaborate in focused breakout groups on Day 2, identifying shared challenges and outlining actionable next steps

Appendix A

Speaker and Panelist Extended Bios

Keynote Speaker

Ray Gabriel

Vice President, Strategic Operations, General Dynamics Electric Boat

Ray Gabriel was named vice president of Strategic Operations of General Dynamics Electric Boat in January 2025. In this role, he is responsible for continuing the company's evolution as a multi-site operation with long-term strategic sourcing partners. He also oversees Electric Boat's operational posture for new program opportunities, including AUKUS and other U.S. Navy initiatives. Ray joined Electric Boat in 2016, following a 32-year career as a submarine naval officer. He holds a master's degree in mechanical engineering from the University of Central Florida and is a graduate of Electric Boat's Business Leader Group (BLG) program.

Panel 1: Power System Resilience and Security

Moderator: Dr. Yan (Lindsay) Sun

University of Rhode Island Professor, ECBE Department Chair, CYPHER Co-Director

Panelist 1: Greg Belanger

Chief Technology Security Officer, PPL Corporation

Greg Belanger joined PPL Corporation in April as Chief Technology Security Officer, where he is leading a strategic modernization of the company's cybersecurity posture, anchored in a vision for the utility of the future. His initiatives include implementing advanced Identity and Access Management systems, deploying cutting-edge application security tooling, establishing a dedicated security architecture practice, and laying the groundwork for a scalable AI security program.

Prior to PPL, Greg spent seven years leading security engineering and architecture for a Fortune 100 commercial real estate firm. His background also includes modernizing cybersecurity operations for a major financial services institution and building a self-service identity management platform from the ground up. A 25-year veteran of agile software development, Greg is passionate about building high-performing, generative teams that drive secure innovation at scale.

Panelist 2: Dr. Esther Amullen

Principal Technical Leader in Cybersecurity, EPRI

Esther M. Amullen, PhD, CISSP, is a cybersecurity and AI expert with a decade of experience applying advanced analytics, machine learning, and security frameworks to critical infrastructure

systems. She currently serves as a Program Lead for Cybersecurity Data and Analytics at the Electric Power Research Institute (EPRI), where she leads innovative research on AI-driven cybersecurity, data management and governance, metrics and Zero Trust architectures for power delivery and operational technology environments.

Prior to her current role, Esther was a Senior Data and Applied Scientist at Microsoft, where she developed cutting-edge AI solutions to detect fraudulent entities, automate decision-making using LLMs, and evaluate assistant performance through comprehensive metrics frameworks. She has a strong track record of building scalable machine learning pipelines, deploying GPT-3/4 integrated systems, and driving measurable impact in high-stakes environments.

Esther's earlier work at EPRI included pioneering a cloud-based cybersecurity metrics platform used across multiple electric utilities and leading development on AI/ML tools for cyber threat detection and resilience. Her contributions span from research at Argonne National Lab and the Information Trust Institute (ITI) at the University of Illinois at Urbana-Champaign (UIUC) to practical deployments of intrusion detection systems in industrial control systems and smart grids.

She holds a PhD and MSc in Computer & Information Systems Engineering from Tennessee State University and a Beng in Telecommunication Engineering from Kyambogo University. A published researcher and a Certified Information Systems Security Professional (CISSP), Esther is passionate about advancing secure, data-driven solutions for critical infrastructure protection.

Panelist 3: Dayne Broderson

Computer and Information Research Scientist, Alaska Center for Energy and Power (ACEP)

Dayne Broderson is the Senior Technologist and Strategic Advisor at the Alaska Center for Energy and Power (ACEP) at the University of Alaska Fairbanks. He is part of ACEP's cross-functional team advancing cyber capacity for energy systems, with a specific focus on integrating students, researchers, and testbed partners into a shared platform for applied learning, research, and technical assistance. Dayne's work spans strategic program development, applied research leadership, and the technical implementation of secure, scalable platforms for modern energy systems. With a background in Computer Science (B.S., UAF), he brings a systems-thinking approach to the intersection of operational technology, cybersecurity, and energy resilience—especially in the context of rural and remote grids.

Dayne leads the coordination of technical assistance efforts with ACEP's energy testbed partners, helping to address technology integration challenges, particularly those involving understanding how to integrate new technologies into legacy systems and operational infrastructure. These real-world engagements inform and shape broader research efforts, aligning cyber-focused innovation with on-the-ground energy needs in Alaska's rural and remote communities.

Dayne holds a B.S. in Computer Science from UAF and brings decades of experience managing resilient research IT platforms, interdisciplinary teams, and large-scale projects across academia, industry, and government sectors.

Panelist 4: Dr. Jennifer Rogers

Cyber Systems Program Chair, US Coast Guard Academy

LCDR Jennifer Rogers is serving as the Cyber Systems Program Chair at the United States Coast Guard Academy in New London, CT, where she leads initiatives to ensure academic curriculum meets CG missions. LCDR Rogers graduated from the U.S. Coast Guard Academy in 2008 with a B.S. in Electrical Engineering and served as an engineer aboard USCGC MIDGETT in Seattle, WA, completing law enforcement and counterdrug patrols in the Eastern Pacific. As part of the Coast Guard Post Graduate Training Program, she earned an M.S. in Electrical and Computer Engineering with a focus on Communications and Signal Processing from Northeastern University in 2012.

Following her graduate studies, LCDR Rogers supported Coast Guard communications systems, overseeing mobile contingency communications assets that provide the Coast Guard and Other Government Agencies with command, control and communications capabilities during emergency and surge operations. Since 2015, she has been a faculty member at the Coast Guard Academy, first as a rotating military faculty, then as a reservist pursuing her Ph.D., and now as a permanently assigned officer. In 2024, she earned a Ph.D. in Electrical Engineering from the University of Rhode Island, focusing on data augmentation for smart grid anomaly detection.

Originally from Plymouth, MA, LCDR Rogers lives in eastern Connecticut with her husband and three children.

Panelist 5: Dr. Hui Lin

Associate Professor, University of Rhode Island, CYPHER Technical Director

Hui Lin is an Associate Professor at the Electrical, Computer, and Biomedical Engineering Department at the University of Rhode Island. He is the technical co-director of the Center for Cyber-Physical Intelligence & Security (CYPHER). He earned his Ph.D. degree in electrical and computer engineering from the University of Illinois at Urbana-Champaign (UIUC) in 2017. His research interests include cybersecurity, intrusion detection systems, and programmable networks in the areas of cyber-physical systems, e.g., power systems and manufacturing systems. He has successfully adapted Zeek (originally known as Bro), a runtime network traffic analyzer, to support network protocols (e.g., DNP3) commonly used in power grid infrastructure. His current work focuses on applying programmable networks (e.g., software-defined networking and P4) and various machine learning methods (graph neural networks and GenAI) to disrupt cyber reconnaissance, increase design flexibility, and reduce mitigation latency in various cyber-physical

security solutions. His research has been sponsored by NSF, DOE, and DOD and he has received NSF CAREER and NSF CRII awards.

Panel 2: Shipyard 4.0

Moderator: Dr. Tim Arcano, Rite-Solutions

Panelist 1: Daniel Reed

Executive Director, Naval Shipbuilding and Advanced Manufacturing Center of Excellence, ATI

Daniel Reed is the Executive Director of the Navy ManTech Naval Shipbuilding and Advanced Manufacturing (NSAM) Center of Excellence. He leads NSAM's operations, team management, project development, and outreach in support of Navy ManTech's mission to advance and deploy manufacturing technologies across U.S. shipyards.

Mr. Reed joined Advanced Technology International in 2021 as Program Manager for both NSAM and the Center for Naval Metal Working. Prior to that, he spent 15 years at General Dynamics NASSCO, the last major new construction shipyard on the U.S. West Coast. There, he was involved in building roughly 30 vessels and managing complex Navy ship repair and modernization projects. His key roles included Manager of Steel Fabrication and Subassembly, Manager of Steel Grandblocking and Erection, and Project Manager in the Navy LHA/LHD Repair Program.

Panelist 2: William Barnes

Chief Information Security Officer, General Dynamics Electric Boat

William Barnes is the Chief Information Security Officer at Electric Boat, where he leads cybersecurity strategy and operations. He brings over 25 years of experience, including two decades as a cybersecurity executive at Pfizer, where he served as Deputy CISO. Earlier, he held leadership roles at Court Square Group, CIGNA, and served as Deputy CIO at Marine Corps Base Quantico. Bill holds degrees from WPI and the Naval War College and is certified as a PMP, CISSP, and PE. He retired as a Colonel in the U.S. Marine Corps Reserves in 2024, having last served as Vice Chief of Staff at Marine Forces Cyberspace Command. He also teaches computer science as an adjunct at Connecticut College and has a deep focus on public-private partnerships, cyber risk reduction, and secure digital transformation.

Panelist 3: Frank Krazer

Systems Engineer, Hexagon Metrology

Frank Krazer is a Systems Engineer at Hexagon Manufacturing Intelligence, where he focuses on integrating and automating industrial metrology equipment in manufacturing. Since 2015, he has worked extensively with 3D coordinate measuring machines and large-volume laser tracker systems. Frank uses precision measurement data to enhance manufacturing quality, throughput,

and path correction. His recent work includes developing IT/OT (Industrial Internet of Things) solutions that connect measurement systems with CNCs, robots, and enterprise software. By bridging gaps between physical manufacturing systems and digital platforms, Frank enables real-time feedback and smarter automation for industrial environments.

Panelist 4: Dr. Manbir Sodhi

Professor, University of Rhode Island, CYPHER Co-Director

Dr. Manbir S. Sodhi is a Professor of Mechanical, Industrial, and Systems Engineering at the University of Rhode Island (URI). He earned his Ph.D. in Industrial Engineering from the University of Arizona and is recognized for his research in optimization, manufacturing systems, and sustainable engineering.

Dr. Sodhi has organized numerous workshops and symposia for defense and industry on topics such as fleet scheduling, smart manufacturing, and digital twins. He has served as department chair and consulted with organizations including NATO, the Naval Undersea Warfare Center, and Submarine Forces Atlantic. His awards include the Carlotti Faculty Excellence Award and the U.S. Navy Summer Faculty Fellowship. Dr. Sodhi's research focus includes cyber-physical systems and digital twins for resilient manufacturing.

Speaker Bios | CUI Session

Keynote Speaker

Dr. Ken Fischer

Chief of Cybersecurity (SSTM), NSWC Philadelphia Division

Keynote Address: Firewalls Can't Stop Flooding: Reframing Cybersecurity for Shipboard Control and Cyber-Physical Systems

Dr. Fischer is serving as NSWCPD's single point of focus for all Hull, Mechanical, and Electrical (HM&E) cybersecurity efforts, including implementation of Risk Management Framework, design and fielding of SABER, development of CVAST, HM&E DevSecOps transition, and leading NSWCPD's cybersecurity R&D efforts.

Previously, Ken served as controls and electrical engineer on a number of programs including the USS Freedom Class, the Egyptian Navy Fast Missile Craft program, and the USS Zumwalt Class. Ken has also served as the Lead Engineer for USS Zumwalt Engineering Control System and as the Controls and Networks Engineering Manager for the Large Surface Combatant.

Ken is a graduate of the University of Delaware with a BS in Chemical Engineering and earned an MS and a PhD in Computer Engineering from Villanova University. Ken authored multiple papers on industrial automation and cybersecurity (focus on cryptography), PLC programming, and quantum computing.

CUI Panel 1: CPS Security and Resiliency Challenges in Shipboard Systems

Moderator: Mr. Paul Boivin

Senior Cybersecurity Engineer, Rite-Solutions, Inc.

Panelist 1: Dr. Ken Fischer

Chief of Cybersecurity (SSTM), NSWCPD [Bio Above]

Panelist 2: Mr. Steve Masterson

Director, Cybersecurity Undersea Warfare (SSTM), NUWCDIVNP

Mr. Masterson is NUWCDIVNPT's Director of Cybersecurity Undersea Warfare (USW), SSTM with over 22 years of experience providing leadership and technical direction in support of combat systems, systems engineering, and cybersecurity. Steve has taken on a wide range of leadership positions in systems engineering and cybersecurity.

Over the past decade, Steve has served as a supervisor and resource manager of cybersecurity personnel, a program manager overseeing the technical implementation of cybersecurity, and the Activity Chief Information Officer (ACIO) overseeing the application of cybersecurity across the portfolio of Command RDT&E enterprise networks. As a supervisor, he oversaw the hiring of dozens of cybersecurity personnel and was instrumental in working with Command leadership to invest in advanced cybersecurity certification training.

Steve received his Bachelor's degree in Computer Engineering and MBA from the University of Rhode Island and currently holds CISSP and CISM certifications.

Panelist 3: Dr. Ben Drozdenko

Cybersecurity S&T Lead, NUWCDIVNPT

Dr. Ben Drozdenko is the NUWCDIVNPT Cybersecurity Science and Technology (S&T) Lead. In this role, he leads Cybersecurity research and development (R&D) projects in the areas of Artificial Intelligence and Machine Learning (AI/ML) for Cyber situational awareness, Cyber-survivability Model-Based Systems Engineering (MBSE), and an ONR-sponsored laboratory project on software de-bloat and hardening.

In his over 20 years of prior experience, he was an Assistant Professor of Cyber Engineering & Computer Science at Louisiana Tech University, a Signal Processing Specialist & Training Engineer at MathWorks, and a Systems Engineer at Raytheon.

Ben's degrees include a Ph.D. in Computer Engineering and an M.S. in Electrical Engineering from Northeastern, and a B.S. in Computer & Systems Engineering from Rensselaer Polytechnic Institute. His certifications include the (ISC)^2 CISSP, SSCP & CCSP and CompTIA Security+.

Panelist 4: Mr. Joe Bransfield

Fleet Cyber Liaison, NUWCDIVNPT

Joe Bransfield, CISSP, MS Cybersecurity (Purdue), retired as NUWC Detachment Command Master Chief in 2021 after a distinguished Navy career. At NUWC, he contributed to Operation Cyber Phoenix and led the Submarine Onboard Readiness Team, training sailors in critical cybersecurity practices. As the current NUWC Fleet Cyber Liaison, he bridges the gap between engineers and submariners, planning and executing cyber tabletop exercises, laboratory testing, and on-platform cybersecurity evaluations. Additionally, as the Science and Technology Intelligence Liaison Officer (STILO), he connects our Division's project teams with the Intelligence Community to address intelligence needs and provides our undersea warfare expertise to the IC.

His previous role as NUWC's Information System Security Manager and Intel Community representative (OPNAV 975) focused on strengthening undersea warfare systems' cyber resilience by identifying countermeasures and providing recommendations for more secure systems.

Passionate about education, Joe teaches cybersecurity (forensics, Linux, ethical hacking) at the Community College of Rhode Island and mentors high school and college cyber competition teams, fostering the next generation of cybersecurity professionals since 2019.

CUI Panel 2: CPS Challenges in Industry 4.0 Shipbuilding, Maintenance, and Repair

Moderator: Dr. Tim Arcano

Chief Technology Officer, Rite-Solutions, Inc.

Panelist 1: Daniel Reed

Executive Director, Naval Shipbuilding and Advanced Manufacturing Center of Excellence, ATI

[Bio Above]

Panelist 2: Michael Chung

CTO, Maritime Technology Group

Michael Chung is the Chief Technology Officer at MTG, with a career spanning startups and major technology firms in the fields of health tech, cybersecurity, and digital transformation. A former U.S. Navy Supply Corps Officer, he served in Operation Enduring Freedom and Operation Iraqi Freedom.

Michael has held key roles at Apple and Microsoft, and was appointed to the Pentagon as part of the 26th Secretary of Defense James Mattis's team, where he led the Department of Defense's Bug

Bounty and ethical hacking initiatives. His expertise includes modernizing cybersecurity strategies across public and private sectors. Michael holds a B.S. in Marine Engineering from the U.S. Merchant Marine Academy and an M.B.A. from the University of Washington.

Panelist 3: Dr. Manbir Sodhi

Professor, University of Rhode Island, CYPHER Co-Director

[Bio Above]

Panelist 4: Wayne Austad

CTO, National & Homeland Security Directorate; Idaho National Laboratory

Mr. Wayne Austad is the Chief Technology Officer for National & Homeland Security at Idaho National Laboratory (INL), where he provides strategic leadership for research, infrastructure, and partnerships supporting critical national security programs. He serves as Chief R&D Officer for CyManII, a DOE-funded institute focused on cybersecurity in automation and supply chains, and leads INL's Secure & Resilient Cyber-Physical Systems Initiative.

With over 30 years at INL, Mr. Austad previously directed the Cybercore Integration Center and founded CyberPARC, a collaborative initiative with PNNL and Sandia. He has led advanced efforts in cyber threat analysis, special programs for defense and intelligence agencies, and the development of INL's Wireless Test Bed. His early work spanned AI, simulation, and SCADA system security.
Mr. Austad holds B.S. and M.S. degrees in Electrical Engineering from the University of Wyoming, specializing in digital signal processing and computer engineering.

Panelist 5: Benjamin Lampe

Cybersecurity Researcher; Idaho National Laboratory

Benjamin Lampe is a Cybersecurity Researcher at the Idaho National Laboratory (INL), specializing in Cyber-Informed Engineering (CIE) since September 2023. At INL, Ben has led R&D into CIE design and implementation methodologies and published several guides and power grid resiliency tools in the CIE national library of materials. His professional journey includes 10 years at the Naval Nuclear Laboratory, where he served as an Operational Technology Enterprise Architect, Systems Analyst, and a Controls Engineer. In these roles, he formulated the OT technical strategy and implemented a nation-wide OT infrastructure between the NNL's process systems. As a Control Engineer, he maintained a myriad of process and monitoring systems within power distribution, water and wastewater management, building automation, and radiological monitoring.