CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

ICSJWG
INDUSTRIAL CONTROL SYSTEMS
JOINT WORKING GROUP

ICSJWG 2023 Spring Meeting Agenda

MAY 9–11 | SALT LAKE CITY, UTAH | RADISSON HOTEL SLC DOWNTOWN

Day 1 – Tuesday, May 9

7:45–8:35 a.m.	**Check-In**	
8:40–9:00 a.m.	**Opening Remarks**	Main
9:00–9:45 a.m.	**Keynote Speaker** CISA Leadership	Main
9:45–10:05 a.m.	**Break**	
9:50–10:50 a.m.	**CDET Instructional Training: Network Discovery – Passive**	C1
10:05–10:50 a.m.	**CDET ICScape – Network Discovery Cyber Escape Room**	C2
10:05–10:50 a.m.	***Do We Have Logs for That? When Network Traffic Analysis Falls Short*** Nikolas Upanavage, Bechtel Corporation Derek LaHousse, Bechtel Corporation	Main
	API 1164 for Enhancing Cybersecurity of Gas Pipeline Operations Ashit Dalal, Capgemini North America	B1
	Generative AI For Detecting Malicious Activity in Physical Infrastructure Jonathan Lee, Nanotronics	B2
10:55–11:55 a.m.	**CDET Instructional Training: Network Discovery – Active**	C1
11:05–11:50 a.m.	**CDET ICScape – Network Discovery Cyber Escape Room**	C2
10:55–11:40 a.m.	***Prioritizing Vulnerability Response Actions Beyond CVE CVSS Base Scores*** Richard Dahl, cmplid:// Inc.	Main
	IoT: Pushing New Boundaries in Security for Industrial Control Systems Benjamin Carter, Center for Internet Security Kaitlin Drape, Center for Internet Security	B1
	Gold Standard Patching Joshua Reber, FoxGuard Solutions	B2
11:40–12:40 p.m.	**Lunch on Your Own**	

12:40–1:40 p.m.	**Vendor Exhibition**	
1:25–2:25 p.m.	**CDET Instructional Training: Network Discovery – Passive**	C1
1:40–2:25 p.m.	**CDET ICScape – Network Discovery Cyber Escape Room**	C2
1:40–2:25 p.m.	***The Emperor Has No Clothes: Where Traditional Incident Response Techniques Come up Wanting in OT Environments*** Bryan Singer, Accenture	Main
	The Importance of Binary Reversing in Network Analysis Javiar Rascon Mesa, Nozomi Networks Roya Gordon, Nozomi Networks	B1
	More Situational Awareness for Industrial Control Systems (MOSAICS) Joint Capability Technology Demonstration (JCTD) Final Results Ross Roley, Battelle Memorial Institute	B2
2:30–3:30 p.m.	**CDET Instructional Training: Network Discovery – Active**	C1
2:30–3:15 p.m.	***Enhancing Cybersecurity of Industrial Control Systems with Digital Watermarking Technology*** Prasad Enjeti, Texas A&M University	Main
	Practical Guidance for Cyber Informed Engineering Tony Turner, Opswright	B1
	OT Monitoring Tools: The Ultimate Guide for Conducting Multi-Vendor Proof-of-Concepts Raphael Arakelian, PwC Canada	B2
2:40–3:25 p.m.	**CDET ICScape – Network Discovery Cyber Escape Room**	C2
3:15–3:35 p.m.	**Break**	
3:35–4:20 p.m.	***Broadening the Scope: Why Non-OT Systems Matter to Operations*** Justin Pascale, Dragos	Main
4:20–4:25 p.m.	**Closing Remarks**	Main
4:25–5:30 p.m.	**Vendor Exhibition**	

Second Floor: Main = Main Room │ B1 = Breakout Room 1 │ B2 = Breakout Room 2
Lobby Level: C1 = Cottonwood 1 │ C2 = Cottonwood 2

Contact us by emailing ICSJWG.Communications@cisa.dhs.gov

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

ICSJWG
INDUSTRIAL CONTROL SYSTEMS JOINT WORKING GROUP

ICSJWG 2023 Spring Meeting Agenda

MAY 9–11 | SALT LAKE CITY, UTAH | RADISSON HOTEL SLC DOWNTOWN

Day 2 – Wednesday, May 10

7:45–8:25 a.m.	**Check-In**	
8:30–8:45 a.m.	**Opening Remarks**	Main
8:45–9:30 a.m.	*Insurance Coverage for ICS - Know Thy Network (And What Can Happen When You Don't)* Miles Carlsen, Carlsen Law Corporation	Main
9:30–9:50 a.m.	**Break**	
9:35–10:35 a.m.	**CDET Instructional Training: Network Discovery – Passive**	C1
9:50–10:35 a.m.	**CDET ICScape – Network Discovery Cyber Escape Room**	C2
9:50–10:35 a.m.	*Developing OT/ICS Cybersecurity Governance Programs for Airport Infrastructures* Zeljko Cakic, Greater Toronto Airports Authority	Main
	Research Reveals: The Complex Threat Landscape of Modern CNCs William Malik, Trend Micro	B1
	Cyber Attacks with Physical Consequences - 2023 Threat Report Andrew Ginter, Waterfall Security Solutions Greg Hale, Industrial Safety and Security Source	B2
10:40–11:40 a.m.	**CDET Instructional Training: Network Discovery – Active**	C1
10:50–11:35 a.m.	**CDET ICScape – Network Discovery Cyber Escape Room**	C2
10:40–11:25 a.m.	*Protecting Industrial Environments from Cyberattacks in Under-Resourced Organizations* Dawn Cappelli, Dragos	Main
	Functional Comparison Between Security Analysis Models (Cyber Kill Chain, STPA-Sec, and OODA) Steve Griffing, Booz Allen Hamilton	B1
	Industrial Cybersecurity Workforce Development Part 1: "The Why" Glenn Merrell, Industrial Control Systems Security	B2
11:25–12:25 p.m.	**Lunch on Your Own**	

12:25–1:25 p.m.	**Vendor Exhibition**	
1:10–2:10 p.m.	**CDET Instructional Training: Network Discovery – Passive**	C1
1:25–2:10 p.m.	**CDET ICScape – Network Discovery Cyber Escape Room**	C2
1:25–2:10 p.m.	***ICS Community Comes Together to Bolster CWE for ICS/OT*** Matthew Luallen, Cybersecurity Manufacturing Innovation Institute ***Physics-Informed Intrusion Detection Using Deep-Packet Inspection of Wind Turbine Control Networks*** Jon Berg, Sandia National Laboratories ***Industrial Cybersecurity Workforce Development Part 2: "The Who"*** Dr. Shane D. Stailey, Idaho National Laboratory Sean McBride, Idaho State University Glenn Merrell, Industrial Control Systems Security	Main B1 B2
2:15–3:15 p.m.	**CDET Instructional Training: Network Discovery – Active**	C1
2:25–3:10 p.m.	**CDET ICScape – Network Discovery Cyber Escape Room**	C2
2:15–3:00 p.m.	***Liberty Eclipse: A Unique Hands-On Cybersecurity Experience*** Jeremy Jones, Idaho National Laboratory Alex Waitkus, Southern Company ***Field-Device-to-Cloud: Using One-Way Isolation to Modernize Remote Asset Monitoring*** Chris Escamilla, Fend Incorporated ***Industrial Cybersecurity Workforce Development Part 3: "The What"*** Sean McBride, Idaho State University	Main B1 B2
3:00–3:20 p.m.	**Break**	
3:20–4:05 p.m.	***Security Truths and Consequences*** Dale Peterson, Digital Bond	Main
4:05–4:15 p.m.	**Closing Remarks**	Main
4:15–5:30 p.m.	**Vendor Exhibition**	

Second Floor: Main = Main Room | B1 = Breakout Room 1 | B2 = Breakout Room 2
Lobby Level: C1 = Cottonwood 1 | C2 = Cottonwood 2

Contact us by emailing ICSJWG.Communications@cisa.dhs.gov

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

ICSJWG
INDUSTRIAL CONTROL SYSTEMS
JOINT WORKING GROUP

ICSJWG 2023 Spring Meeting Agenda

MAY 9–11 | SALT LAKE CITY, UTAH | RADISSON HOTEL SLC DOWNTOWN

Day 3 – Thursday, May 11

7:45–8.25 a.m.	**Check-In**	
8:30–8:35 a.m.	**Opening Remarks**	Main
8:35–9:20 a.m.	***Regulation is Coming: What's Going on in Europe?*** Jens Wiesner, German Federal Office for Information Security (BSI)	Main
9:25–10:10 a.m.	***Hypothesis-Driven Approach to Threat Hunting*** David Hudson, Idaho National Laboratory	Main
	Cyber Resiliency Analysis of Critical Functions – Initial Access/Remote Access Analysis Across Critical Infrastructure Sectors Adam Hahn, The MITRE Corporation Marie Collins, The MITRE Corporation	B1
	Open-Source Security Software Usage in Industrial Secure Software Development Lifecycles Ronald Bondy, Aveva	B2
10:10–10:30 a.m.	**Break**	
10:15–11:15 a.m.	**CDET Instructional Training: Network Discovery – Passive**	C1
10:20–11:05 a.m.	**CDET ICScape – Network Discovery Cyber Escape Room**	C2
10:30–11:15 a.m.	***Malcolm: Not Just Another Pretty Monitoring Tool; Ingesting Endpoint Logs with Fluent Bit*** David Conner, Idaho National Laboratory	Main
	Human Considerations in ICS/OT Cybersecurity Incident Response Susan Howard, Michael Baker International Fred Gordy, Michael Baker International	B1
	Insights Into the Vulnerability Management Process Nathan Dunn, Idaho National Laboratory	B2
11:20–12:20 p.m.	**CDET Instructional Training: Network Discovery – Active**	C1
11:20–12:05 p.m.	**CDET ICScape – Network Discovery Cyber Escape Room**	C2

11:20–12:05 p.m.	*Cyber Performance Goals (CPG) Module Within CSET* Barry Hansen, Idaho National Laboratory	Main
	A Systematic and Practical Approach to Securing ICS/OT Jeff Watts, RPI Group James Mahoney, US Marine Corps	B1
	Zero Trust Policy Design for Industrial Control Systems Dr. Jens Meggers, Mission Secure	B2
12:05–1:05 p.m.	**Lunch on Your Own**	
1:05–1:50 p.m.	*Understanding the Need for Industrial Cyber Workforce Development* Dr. Shane D. Stailey, Idaho National Laboratory	Main
1:50–2:05 p.m.	**Closing Remarks**	Main
2:05–3:00 p.m.	**Vendor Exhibition**	

Main = Main Room │ B1 = Breakout Room 1 │ B2 = Breakout Room 2
Lobby Level: C1 = Cottonwood 1 │ C2 = Cottonwood 2