GRIDSECCON 2019

NERC • SERC

October 22–25

Westin Peachtree Plaza
210 Peachtree Street NW
Atlanta, GA 30303

Welcome Letter

Welcome to our ninth annual grid security conference, GridSecCon 2019!

For the second year, NERC is co-hosting GridSecCon with a Regional Entity—the SERC Reliability Corporation (SERC)—as part of the Electric Reliability Organization (ERO) Enterprise's collaborative efforts to protect the North American bulk power system (BPS) through information sharing, education, and collaboration. Electricity is foundational to modern society, and NERC and the Regional Entities seek to be a critical part of the reliability and security fabric of the North American electric industry.

GridSecCon is the ERO Enterprise's marquee event to bring together security professionals to discuss threats and solutions to help enhance our protection efforts. Security and reliability are inextricably linked, and events like GridSecCon help us plan and prepare for contingencies through training, information sharing, and lessons learned. To be successful, we must build a "collective defense" to avoid, mitigate, and solve our critical security challenges.

NERC's Electricity Information Sharing and Analysis Center (E-ISAC) seeks to be an essential part of enhancing these efforts. The E-ISAC not only helps educate industry about threats and solutions but works to strengthen the cyber and physical security of our grid.

This year, we're excited to welcome you to Atlanta—NERC's headquarters and a major city in SERC's geographic footprint. Keynotes from leaders at Southern Company, the U.S. Department of Energy (DOE), and the U.S. Department of Homeland Security (DHS) and other industry leaders are planned. We appreciate these leaders taking time from their busy schedules to share their insights on the latest strategies and solutions to handle cyber and physical security threats.

The agenda also includes panel discussions on electricity and natural gas interdependencies, supply chains, the current threat landscape, GridEx V planning, and game-changing research and development (R&D). We'll also hear from four trade associations in the United States and Canada to learn how we can better leverage these groups to support our security efforts. Security providers will discuss solutions on how to defend against threats to the grid, and the conference will culminate with threat briefings and tours of area security centers.

We know our industry is strong and takes security risks seriously, but we must remain vigilant as our adversaries continue to develop more sophisticated campaigns that place the North American grid at risk. This is why a learning environment like GridSecCon is increasingly important. We cannot ensure reliability without also ensuring the security of the North American BPS. GridSecCon is one way that the ERO Enterprise fosters a learning environment that supports this common goal. We look forward to the discussions and a successful conference.

Jim Robb
President and Chief Executive Officer
North American Electric Reliability Corporation

Jason Blake
President and Chief Executive Officer
SERC Reliability Corporation

Agenda

For maps of event locations, see pages 35–37.

Monday, October 21 | Preconference

6:00–8:00 p.m. **Evening Registration (no reception)**

Terrace, Eighth Floor

Tuesday, October 22 | Training Day

7:00 a.m.–5:00 p.m. **Registration**

Terrace, Eighth Floor

7:00–8:00 a.m. **Continental Breakfast**

Augusta Foyer, Seventh Floor

Terrace, Eighth Floor

8:00 a.m.–12:00 p.m. **Morning Sessions**

	Training Tracks	Training Provider	Location
1A	Grid NetWars Tournament	The SANS Institute (SANS)	Peachtree D Eighth Floor
2A	Physical Security Workshop I	E-ISAC Physical Security Partners	Peachtree C Eighth Floor
3A	Creating a Consequence-Based Tabletop Exercise	Dragos	Augusta G Seventh Floor
4A	Exercise Chaos Management	Tennessee Valley Authority (TVA)	Augusta H Seventh Floor
5A	Securing the Supply Chain	Deloitte	Augusta E/F Seventh Floor
6A	Measuring, Communicating, and Quantifying Cyber Risk	Axio	Augusta C/D Seventh Floor

12:00–1:00 p.m. **Lunch**

Savannah Ballroom, Tenth Floor

1:00–5:00 p.m. **Afternoon Sessions**

	Training Tracks	Training Provider	Location
1B	Grid NetWars Tournament	SANS	Peachtree D Eighth Floor
2B	Physical Security Workshop II	E-ISAC Physical Security Partners	Peachtree C Eighth Floor
3B	Risky Business: Governance, Risk, and Compliance without Threat Intelligence	Dragos	Augusta G Seventh Floor
4B	Reducing Human Error in Cyber Event Response	ResilientGrid Inc.	Augusta H Seventh Floor
5B	Five Blind Men and the Elephant called Supply Chain Security: Effective Management of Software Supply Chain Security	aDolus Inc.	Augusta E/F Seventh Floor
6B	Secure Operations Technology Advanced Cyber Security Training	Waterfall Security Solutions	Augusta C/D Seventh Floor

5:30–8:30 p.m. **Welcome and Networking Reception** *(Sponsored by Force5, Inc.)*
Augusta Conference Center, Seventh Floor

Wednesday, October 23 | Strategies and Threat Day

7:30 a.m.–5:00 p.m. **Registration**
Terrace, Eighth Floor

7:30–8:30 a.m. **Continental Breakfast** *(Sponsored by OWL Cyber Defense)*
Exhibitor Hall (Augusta Conference Center, Seventh Floor)

8:30–8:45 a.m. **Introductory Remarks, Logistics, and Safety Briefing**
Bill Lawrence, Vice President and Chief Security Officer (CSO), NERC
Peachtree Ballroom, Eighth Floor

8:45–9:00 a.m. **Welcome Address and Opening Keynote**
Jim Robb, President and Chief Executive Officer (CEO), NERC
Peachtree Ballroom, Eighth Floor

9:00–9:15 a.m. **Energy Keynote**
The Honorable Karen S. Evans, Assistant Secretary, Office of Cybersecurity, Energy Security, and Emergency Response (CESER), U.S. DOE
Peachtree Ballroom, Eighth Floor

9:15–9:30 a.m.

Homeland Security Keynote

The Honorable Brian M. Harrell, Assistant Director, Infrastructure Security Division, U.S. Cybersecurity and Infrastructure Security Agency (CISA), U.S. DHS

Peachtree Ballroom, Eighth Floor

9:30–9:45 a.m.

CEO Keynote

Tom Fanning, Chair, President and CEO, Southern Company

Peachtree Ballroom, Eighth Floor

9:45–10:00 a.m.

Regional Entity Keynote

Brian Thumm, Vice President, Performance Improvement and Risk Management, SERC

Peachtree Ballroom, Eighth Floor

10:00–10:30 a.m.

Break *(Sponsored by Burns & McDonnell)*

Exhibitor Hall (Augusta Conference Center, Seventh Floor)

10:30–11:15 a.m.

Advocating for Security: Behind-the-Scenes Look at Trade Associations *(panel discussion)*

Moderator: Sharla Artz, Senior Vice President, Government Affairs, Utilities Technology Council (UTC)

Bridgette Bourge, Director, Legislative Affairs, National Rural Electric Cooperative Association (NRECA)

Francis Bradley, President and CEO, Canadian Electricity Association (CEA)

Nathan Mitchell, Senior Director, Cyber and Physical Security Services, American Public Power Association (APPA)

Laura Schepis, Senior Director, National Security, Edison Electric Institute (EEI)

Peachtree Ballroom, Eighth Floor

11:15 a.m.–12:00 p.m.

Design Basis Threat (DBT) Assessment *(panel discussion)*

Moderator: Michael Bowen, Associate Director, Physical Security, E-ISAC

David Godfrey, Critical Infrastructure Protection Manager, Garland Power & Light (GP&L)

David Jarrett, Senior Advisor, Physical Security, Southern California Edison (SCE)

Peter Scalici, Manager, Security Outreach Programs, Northeast Power Coordinating Council

Peachtree Ballroom, Eighth Floor

12:00–1:15 p.m.

On-Site Lunch *(Sponsored by Tripwire)*

Whitehall, Sixth Floor

1:15–2:00 p.m.

Unmanned Aircraft System (UAS) Response Procedures *(panel discussion)*

Moderator: Travis Moran, Vice President, Operations, Welund North America

Kevin Berent, Technical Executive, Power Delivery and Utilization – Transmission, Electric Power Research Institute (EPRI)

L. Scott Parker, Deputy Branch Chief, Risk Mitigation and Strategic Innovation, Security Programs – Infrastructure Security Division, CISA, U.S. DHS

Peachtree Ballroom, Eighth Floor

2:00–2:45 p.m.

When Cyber Attacks Have Physical Effects *(panel discussion)*

Moderator: Jeff Jones, Manager, Industrial Cyber Security, E-ISAC

Amy Bejtlich, Senior Adversary Hunter, Dragos

Sam Chanoski, Director, Intelligence, E-ISAC

Tim Conway, Technical Director, Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) Programs, SANS

William (Bill) Peterson, Manager, Entity Outreach and Training, SERC

Peachtree Ballroom, Eighth Floor

2:45–3:15 p.m.

Break *(Sponsored by Dragos)*

Exhibitor Hall (Augusta Conference Center, Seventh Floor)

3:15–4:00 p.m.

Supply Chain Threat Vector *(panel discussion)*

Moderator: Tom Alrich, Principal Consultant, Tom Alrich LLC

Howard Gugel, Vice President, Engineering and Standards, NERC

François Lemay, Cyber Security Specialist, Hydro-Québec

Brian Owen, Cyber Security Manager, OSISoft

David (Dave) E. Whitehead, Chief Operating Officer (COO), Schweitzer Engineering Laboratories (SEL)

Virginia (Ginger) Wright, Energy-Cyber Portfolio Manager, Cybercore, Idaho National Laboratory (INL)

Peachtree Ballroom, Eighth Floor

4:00–5:00 p.m.

Future Threats—What Comes Next? *(panel discussion)*

Moderator: Sam Chanoski, Director, Intelligence, E-ISAC

Ben Blakely, Vice President, Chief Security Officer (CSO), Hydro One Networks, Inc.

Ann Delenela, Vice President, Information Security, Entergy

Ben Miller, Vice President, Professional Services and R&D, Dragos

Zachary (Zach) Tudor, Associate Laboratory Director, National and Homeland Security, INL

Peachtree Ballroom, Eighth Floor

5:00 p.m.

Tribute to Mike Assante

Tim Conway, Technical Director, ICS and SCADA Programs, SANS

Peachtree Ballroom, Eighth Floor

5:30–8:30 p.m.

Evening Networking Reception *(sponsored by Certrec)*

Exhibitor Hall (Augusta Conference Center, Seventh Floor)

Thursday, October 24 | Solutions Day

7:30–8:30 a.m.

Continental Breakfast
Exhibitor Hall (Augusta Conference Center, Seventh Floor)

8:30–9:15 a.m.

Building a Cyber Threat Model and Coordinating Cyber Threat Intelligence *(panel discussion)*

Moderator: Jeff Jones, Manager, Industrial Cyber Security, E-ISAC

Amy Batallones, Cyber Security Operations Center Manager, Con Edison

Kurt Hoffmann, Information Security Program Adviser, Berkshire Hathaway Energy

Tabice Ward, Director, Information Protection and Security, Chief Information Security Officer (CISO), DTE Energy

Peachtree Ballroom, Eighth Floor

9:15–10:00 a.m.

Game-Changing Research, Development, and Deployment *(panel discussion)*

Moderator: Hailey Siple, Manager, National Security Policy, EEI

Otis Alexander, Lead Cyber Security Engineer, MITRE

Cynthia Hsu, Cybersecurity Program Manager, Business and Technology Strategies, NRECA

Matthew (Matt) Wakefield, Director, Information and Communications Technology R&D, EPRI

Peachtree Ballroom, Eighth Floor

10:00–10:30 a.m.

Break *(sponsored by Cooper Compliance)*

Exhibitor Hall (Augusta Conference Center, Seventh Floor)

10:30–11:30 a.m.

Natural Gas Interdependencies *(panel discussion)*

Moderator: Matt Duncan, Manager, Policy and Coordination, E-ISAC

Kathy Judge, Head of U.S. Physical Security, National Grid

Tamara Lance, Director of Information Security, Atmos Energy

Suzanne Lemieux, Manager, Midstream and Industry Operations, American Petroleum Institute

Robert Mims, Director, Security – Gas, Nuclear, and Electric Security Operations, Southern Company

Peachtree Ballroom, Eighth Floor

11:30 a.m.–12:45 p.m.

On-Site Lunch

The Cellar, Sixth Floor

12:45–2:30 p.m.

Lightning Round of Security Solutions

Peachtree Ballroom, Eighth Floor

Cyber Resilience Metrics

Ray Sefchik, Director, Reliability Assurance, ReliabilityFirst

High-Frequency Radio for Contingency Communications

David Rudawitz, Critical Infrastructure Advisor, NVIS Communications, LLC

Using Maturity Matrices to Evaluate Your Physical Security Program and Improve Your Security Posture

Jason Ivall, Program Manager, Infrastructure Protection and Security, the Centre for Energy Advancement through Technological Innovation (CEATI) International

Protecting Grid Infrastructure with Blockchain Technology

Roman Arutyunov, Co-Founder, Vice President, Products, Xage Security

Power Plants, Trains, and Dishwashers: Third-Party Code Is Everywhere

Jake Kouns, CISO and COO, Risk Based Security

Practical Penetration Testing for Industrial Control Systems

John Biasi, Senior Cyber Security Specialist, Burns & McDonnell

Harnessing the Power of Thermal Cameras and Edge Analytics

Michael Chaffee, Director, Sales, Security, FLIR Systems, Inc.

Supply Chain Risk Management

Carter Schoenberg, Executive Vice President, Cyber Security Solutions, IP Keys

Future Proofing Security, Safety, and Data Privacy in the Age of Digital Transformation

Reeji Booj, Director, Marketing, Alert Enterprise

2:30–3:00 p.m.

Break

Exhibitor Hall (Augusta Conference Center, Seventh Floor)

3:00–4:00 p.m. **Physical Security Outlook** *(panel discussion)*
Moderator: Kristen Bove, Principal Analyst, Physical Security, E-ISAC
Mike Almeyda, Physical Security Subject Matter Expert, Security and, Force5, Inc.
Ross Johnson, President, Bridgehead Security Consulting, Inc.
Kristen Worosz, Senior Analyst, Welund
Peachtree Ballroom, Eighth Floor

4:00–5:00 p.m. **GridEx V** *(panel discussion)*
Moderator: Jake Schmitter, Senior Manager, Training and Exercises, E-ISAC
Stuart Brindley, President, S.J. Brindley Consulting, Inc.
Dustin Cornelius, End Point Security Principal, Southern Company Transmission Energy Management System
Tami B. Fowler, Senior Program Manager, Emergency Preparedness, TVA
Sam Rozenberg, Engineering Services Security Director, APPA
Peachtree Ballroom, Eighth Floor

5:00 p.m. **GridSecCon 2019 Closing Comments**
Bill Lawrence, Vice President and CSO, NERC
Peachtree Ballroom, Eighth Floor

Friday, October 25 | Tours and Briefings Day

The threat briefing, classified briefing, and two tours require advanced registration and confirmation.

7:30–8:00 a.m. **Continental Breakfast**
Terrace, Eighth Floor

8:00–9:30 a.m. **Threat Briefing—For Official Use Only**
Peachtree Ballroom, Eighth Floor

9:30–10:00 a.m. **Prebrief for Mercedes-Benz Stadium Tour**
Peachtree Ballroom, Eighth Floor

10:15 a.m.–12:00 p.m. **Classified Briefing** *(secret clearance required | transportation provided)*

10:15 a.m.–1:30 p.m. **Secureworks Tour** *(transportation provided)*

10:15 a.m.–12:30 p.m. **Mercedes-Benz Stadium Tour** *(transportation provided)*

Training Track Descriptions

Track 1A and 1B: Grid NetWars Tournament
SANS
All-day, 200 seats available, starts at 8:00 a.m.
Audience: Operational technology (OT) security professionals

Grid NetWars is a suite of hands-on, interactive learning scenarios that enable OT security professionals to develop, test, and master the real-world, in-depth skills they need to defend real-time systems. It is designed as a challenge competition and is split into separate levels that allow players to quickly move through earlier levels based on their expertise. The Grid NetWars experience has been themed for the electricity industry, and the scenario has been previously used to support multiple electricity sector exercises. Grid NetWars was designed to enable participation by players at all skill levels and from any sector.

Track 2A: Physical Security Workshop I
E-ISAC Physical Security Partners
Half-day, 200 seats available, starts at 8:00 a.m.
Audience: Physical security professionals, asset owners and operators (AOOs)

This training session will explore issues that affect the physical security of the electricity industry. Participants will hear about current issues and best practices from physical security experts from a variety of perspectives and dialogue with security professionals about concerns. This track includes a panel discussion on insider threat, a presentation on an augmented reality pilot, and a briefing from the National Crime Information Center for Infrastructure Facilities.

Track 2B: Physical Security Workshop II
E-ISAC Physical Security Partners
Half-day, 200 seats available, starts at 1:00 p.m.
Audience: Physical security professionals, AOOs

This training will include presentations from the National Counterterrorism Center (discussing incidents of terrorism that have impacted the energy sector), the U.S. FBI (on physical security threats), and on an introduction to tools available to aid in assessing physical security systems. This suite of tools is the electricity industry DBT and the DBT Implementation Guide, which assists users in applying the DBT to their facilities using the Vulnerability to Integrated Security Analysis methodology.

Track 3A: Creating a Consequence-Based Tabletop Exercise
Dragos Inc.
Half-day, 45 seats available, starts at 8:00 a.m.
Audience: Cyber security professionals

This three-part training will focus on establishing exercise goals and objectives, creating custom exercise scenarios, and conducting a thorough tabletop exercise. At the conclusion of the training, participants will walk through the selection of exercise objectives, creation of an environment-specific scenario, attack artifacts and injects, and what should be captured during the evaluation of game play.

Track 3B: Risky Business: Governance, Risk, and Compliance without Threat Intelligence
Dragos Inc.
Half-day, 45 seats available, starts at 1:00 p.m.
Audience: Cyber security professionals

Governance, risk, and compliance standards struggle to keep up with a rapidly changing world. In cyber security, this is more apparent when reviewing compliance standards, risk models, and overall governance because of serious gaps in standards versus security. Threat intelligence is a way to bridge the gap between minimum baselines and advanced state actors. It helps defenders and policy makers understand what they are really up against, providing for better knowledge and defensive postures. More standards and frameworks are warming up to the use of threat intelligence, but examples from the real world need to be baked into your threat model. Participants will learn how a more complete picture of current threats helps exceed current governance, risk, and compliance standards.

Track 4A: Exercise Chaos Management
TVA
Half-day, 40 seats available, starts at 8:00 a.m.
Audience: Open to all

This session will focus on the elements GridEx exercise planners and controllers will run into during the exercise. It provides guidance on how to handle problems and resolve unforeseen issues that arise during the exercise. This course walks the students through delivering injects, crafting on-the-spot injects, player engagement, controlling the flow the game, capturing lessons learned, building the after-action report, and effectively crafting improvements to gain management support. This exercise will cover cyber security, physical security, and operational injects and experiences, and will demonstrate how to take a standard inject and make it more exciting and engaging for the players.

Participants will leave the session with a GridEx V exercise plan, a set of tabletop scenarios developed by the trainer, and a sample pack of network maps and corresponding city maps (i.e., game boards) that they can use in their exercises.

Track 4B: Reducing Human Error in Cyber Event Response
ResilientGrid Inc.
Half-day, 40 seats available, starts at 1:00 p.m.
Audience: Open to all

Several factors come together when an organization is responding to a cyber event and people are under extreme stress, making rapid decisions, and at increased risk of making errors. This training covers several areas of human factors around reduction of human error in high-stakes situations, including identification and mitigation of cognitive bias, organizational factors that increase resiliency, and human perceptual limitations that can be built into system design to increase the likelihood of intended outcomes.

The learning objective for this session is to increase understanding of human factors in emergency response and how design decisions (systems, organizational, and individual) can reduce risks of human errors.

Track 5A: Securing the Supply Chain
Deloitte
Half-day, 80 seats available, starts at 8:00 a.m.
Audience: Cyber security and information technology professionals

China, Russia, and other potential adversaries are ramping up their efforts to corrupt the supply chains on which the electric grid and other infrastructure sectors depend. The U.S. intelligence community warns that the growing scale and sophistication of attacks on the supply chain "are placing entire segments of our government and economy at risk." The U.S. DHS, U.S. DOE, and other agencies highlight the degree to which supply chain exploitation efforts are metastasizing and becoming ever-more difficult to detect. The U.S. DHS established the Information and Communication Technology Supply Chain Risk Management (SCRM) Task Force in 2018. The U.S. Federal Energy Regulatory Commission (FERC) approved Critical Infrastructure Protection (CIP) Reliability Standard CIP-013-1 to mitigate cyber security risks to the reliable operation of the Bulk Electric System by implementing security controls for SCRM. FERC mandates that electric power and utilities comply with new CIP-013-1 requirements by July 1, 2020. While regulation intends to address cyber security supply chain risks through mandatory compliance requirements, this presentation is a streamlined approach to SCRM through community collaboration among key industry participants and suppliers. This training will also cover lessons learned from a leading energy provider implementing SCRM security controls.

Track 5B: Five Blind Men and the Elephant called Supply Chain Security: Effective Management of Software Supply Chain Security
aDolus Inc.
Half-day, 80 seats available, starts at 1:00 p.m.
Audience: Cyber security and IT professionals

Are participants' software and firmware supply chains compliant with NERC Reliability Standard CIP-013-1? What exactly does securing the software supply chain really involve? This training session will discuss four key risks to software and firmware supply chains in the power industry and provide specific examples of each of these threats. It will then introduce the Framework for Analysis and Coordinated Trust—a framework funded by the U.S. DHS Silicon Valley Innovation Program to safeguard against ICS supply chain attacks.

We will show how to demonstrate compliance with the following CIP-013-1 requirements without introducing onerous, costly, or error-prone processes:

- Verification of software integrity and authenticity: Learn how to ensure that staff members are not loading counterfeit or tampered software and firmware into critical systems.
- Vulnerability detection and disclosure: Learn how to generate a software bill of materials to reveal unexpected or unapproved sub-components that may contain vulnerabilities or malware.

In addition to NERC requirements, we will explore how to address additional supply chain risks:

- Validation of firmware versions: Learn how to ensure that firmware is up-to-date, tested, and approved by the factory rather than an unauthorized or obsolete version.

- Validation of certificate chains: Learn how to detect fraudulently signed packages masquerading as authentic, avoiding Stuxnet-style attacks where private keys have been stolen.

Today's application program interface and web tools allow end users to incorporate validation processes into their daily operations without impeding critical operation, ensuring the legitimacy of updated firmware and software.

Track 6A: Measuring, Communicating, and Quantifying Cyber Risk
Axio
Half-day, 80 seats available, starts at 8:00 a.m.
Audience: Open to all

Risk management is part of our daily lives as utility operators, but what are the best practices for addressing cyber security risk? Regardless of NERC CIP and other regulations, how can participants' utility effectively measure and communicate on cyber risk outside of "red, yellow, or green?" Learn how to identify and assess a wide variety of cyber and physical security risks with limited resources in a utility environment. This workshop will guide participants through how risk is traditionally defined and then provide a best-in-class technique used across industry to quantify—in dollars and cents—the impacts associated with cyber security. This methodology has been used by hundreds of organizations to link the chief financial officer to the CISO and is the one metric that can provide increased budget, resources, and board-level visibility.

Participants can apply lessons learned from this workshop to improve risk management within their organizations immediately. Professionals with different expertise are welcome! As an added bonus, participants will be given tools to help quantify the upcoming GridEx V scenario for management debriefs so they can ultimately answer the question, "Now that we've done that exercise, how bad would the damage have been?"

Track 6B: Secure Operations Technology Advanced Cyber Security Training
Waterfall Security Solutions
Half-day, 80 seats available, starts at 1:00 p.m.
Audience: Cyber security professionals

This course surveys industrial network security problems and introduces secure operations technology (SEC-OT)—a perspective methodology and set of best practices for designing secure ICS. SEC-OT is the methodology used by the world's most secure industrial sites. What the most secure sites do differs sharply from what most industrial sites do. This course is based on the instructor's latest book, *Secure Operations Technology*. Free copies of the book will be available to participants courtesy of Waterfall Security Solutions.

Tour Descriptions

Secureworks

Secureworks is a technology-driven cyber security leader that protects organizations in the digitally connected world. Built on proprietary technologies and world-class threat intelligence, Secureworks applications and solutions help prevent, detect, and respond to cyber threats. Red Cloak software brings advanced threat analytics to thousands of customers, and the Secureworks Counter Threat Platform processes more than 300 billion threat events per day. Secureworks understands complex security environments and is passionate about simplifying security with Defense in Concert so that security becomes a business enabler. More than 4,000 customers across over 50 countries are protected by Secureworks, benefit from the network effect, are collectively smarter, and exponentially safer.

Mercedes-Benz Stadium

Opened in August 2017, Mercedes-Benz Stadium is a world-class sports and entertainment venue in downtown Atlanta and home to the National Football League's Atlanta Falcons and Major League Soccer's Atlanta United. The multi-purpose stadium hosts major sports and entertainment events—including the 2018 College Football Playoff Championship game, the Super Bowl in 2019, and the NCAA Men's Final Four in 2020. It is also the first professional sports stadium in North America to achieve Leadership in Energy and Design Platinum Certification by the United States Green Building Council. Mercedes-Benz Stadium is proud to be collaborating with nearly a dozen founding partners, including Coca-Cola, Equifax, The Home Depot, NCR, Novelis, SCANA Energy, SunTrust, IBM, Georgia Power, and American Family Insurance.

Speaker Profiles

Sharla Artz
Senior Vice President, Government Affairs and Cybersecurity
UTC

Sharla Artz is the senior vice president of Government Affairs and Cybersecurity for UTC and focused on cross-sector interdependencies in CIP. Ms. Artz supports the electricity sector's communications for a resilient electric grid and serves as a member of the Communications Sector Coordinating Council and the Critical Manufacturing Sector. Her work in these government and private sector partnerships provides cross-sector situational awareness to UTC's electric, natural gas, and water utility members.

She was the director of Government Affairs at SEL, a critical equipment supplier focused on ICS security. Ms. Artz was also the assistant general counsel for the National Association of Regulatory Commissioners, serving state utility commissioners. After receiving her juris doctor from Georgetown University, Ms. Artz worked for a member of the U.S. Congress' House Energy and Commerce Committee.

Roman Arutyunov
Co-Founder and Vice President of Products
Xage

Roman Arutyunov is the co-founder and vice president of Products at Xage. Mr. Arutyunov leads the Product Vision and Go-to-Market teams at Xage with experience in security, networking, and industrial applications. Prior to Xage, he spent 15 years in roles as vice president of Product and Engineering at ABB, Tropos Networks, and Mimosa Networks, where he solved networking, security, and data analytics challenges for industrial and commercial enterprises, enabling millions of Internet of Things devices in production today. Earlier in his career, Mr. Arutyunov worked on the first generation of content distribution networks and proxy servers at Blue Coat Systems (Symantec). Mr. Arutyunov has a bachelor's degree in Applied Mathematics with an emphasis in computer science from the University of California, Berkeley, and a master's degree in Business Administration from Columbia University.

Amy P. Batallones
Cyber Security Operations Center Manager
Con Edison

Amy Batallones is manager of the Cyber Security Operations Center at Con Edison Company of New York. Ms. Batallones leads the team responsible for 24/7 analysis and response to cyber security threats to the company. She previously worked in information security risk management, designing secure architectures for IT and OT systems, conducting vulnerability and risk assessments, and drafting cyber security policies. Ms. Batallones previously served as a member of the Executive Committee for IEEE's New York Section and is an adjunct professor at Fordham University.

Ms. Batallones has a bachelor's degree in Computer Science from Fordham University and a master's degree in Management of Technology from New York University.

Kevin Berent
Technical Executive, Power Delivery and Utilization – Transmission
EPRI

Kevin Berent is a technical executive of Power Delivery and Utilization – Transmission at EPRI. His current work is focused on transmission and substations and includes topics such as resiliency, countering the drone threat, and physical security. Some of Mr. Berent's previous projects centered on sulfur hexafluoride (SF6) and its alternatives.

Prior to EPRI, Mr. Berent was a director at the North American Transmission Forum and a manager at SERC. For eight years, he focused on improving the reliability and resiliency of the BPS in the United States and Canada. He brings a diverse leadership background including manufacturing and industrial engineering (at Michelin), service and sales (at Cintas), and military service (as a navigator in the U.S. Air Force).

Mr. Berent earned a bachelor's degree in Management from the U.S. Air Force Academy. Additionally, he has a master's degree in Operations Management from the University of Arkansas and a master's degree in Business Administration from the University of South Carolina.

John Biasi
Senior Cyber Security Specialist
Burns & McDonnell

John Biasi is a technical lead with the Compliance and Critical Infrastructure Protection department within Burns & McDonnell. He is an accomplished professional with notable success directing a broad range of IT and cyber security initiatives while participating in planning, analysis, and implementation of solutions in support of business objectives. Mr. Biasi has hands-on experience developing solutions for a broad range of regulations and security frameworks, including the Health Insurance Portability and Accountability Act, International Organization for Standardization 27001, Nuclear Energy Institute 08-09, NERC CIP Standards, National Institute of Standards and Technology, Payment Card Industry Data Security Standard, and the Sarbanes-Oxley Act. Mr. Biasi has several cyber security certifications, including Certified Information Systems Security Professional (CISSP), Certified Information Security Auditor (CISA), and Certificate of Cloud Security Knowledge. He also has a master's degree in Business Administration with a concentration in Cyber Security Management. Mr. Biasi has worked in the utility industry for more than 10 years and in cyber security for nearly 20 years.

Bridgette Bourge
Director, Legislative Affairs
NRECA

As director for homeland security issues at NRECA, Bridgette Bourge brings more than 20 years of expertise leading policy and advocacy at the nexus of public–private critical infrastructure within local and state governments, Congress, and federal agencies. Before joining NRECA in January 2014, Ms. Bourge served as a consultant to the U.S. DHS on cyber security CIP in addition to having worked previously in the financial and chemical sectors. She understands the challenges of ensuring critical infrastructure security from both the private and public sector perspectives.

Ms. Bourge supports the efforts of electric cooperative leaders to maintain and boost their coops' ability to supply safe, affordable, and reliable electricity to members. She provides information and directs advocacy on the intricate technical aspects of the electric grid and distribution system security to congressional offices that craft federal policies to support and protect those systems. Working directly with the private sector, agencies, and Congress, Ms. Bourge helps electric cooperatives engage and address issues impacting national security and response capabilities, electricity industry recovery, and homeland and local security.

Ms. Bourge brings unique operational understanding and insight into public and private sector requirements and procedures and practices as well as real-world knowledge of the common goals of both to ensure a more resilient electricity sector across the country.

Kristen Bove
Principal Analyst, Physical Security
E-ISAC

Kristen Bove is a principal analyst for the E-ISAC and is focused on physical security analysis. She directly engages with AOOs on a daily basis to provide high-quality, timely, reliable analysis and context regarding physical security and industry trends, emerging tactics, techniques, procedures, and relevant threat actor behaviors. Ms. Bove's prior experience includes working as an analyst for the U.S. DHS's Office of Infrastructure Protection, where she was responsible for developing and implementing national risk mitigation programs primarily focused on the energy sector.

Ms. Bove has worked with a variety of public and private sector organizations to provide strategic analysis and risk management solutions for critical infrastructure. She has a bachelor's degree in History from Arizona State University and a master's degree in Politics, Security, and Integration from University College London.

Michael Bowen
Associate Director, Physical Security
E-ISAC

Michael Bowen is an associate director of physical security at the E-ISAC. Mr. Bowen directs and develops physical security initiatives and analysis for the entire North American power grid.

Prior to joining the E-ISAC, Mr. Bowen worked at the U.S. DHS, where he was the program manager for the Critical Infrastructure Information Sharing Environment—the sector-specific agency representative for both the chemical and dams sectors. Mr. Bowen has a bachelor's degree in Business Administration from Upper Iowa University and is a graduate of the U.S. Army Sergeants Major Academy.

Steven Briggs
Senior Program Manager
TVA

Steven Briggs has worked for TVA for 10 years and is currently serving as a senior program manager responsible for the cyber security of TVA's coal, natural gas, and hydro fleets. He is a NERC CIP subject matter expert focusing on vulnerability management and incident response.

Mr. Briggs is an active member of the NERC Critical Infrastructure Protection Committee (CIPC) Supply Chain Working Group, facilitating the team's writing of the *Vendor-Identified Incident Guideline*. He co-led the cyber team for the GridEx Working Group (GEWG) for GridEx III and IV, and he has worked to advance TVA's and the utility sector's emergency response processes and adoption of Federal Emergency Management Agency (FEMA) ICS principles. Mr. Briggs is a supporter of multiple efforts for CIP.

Mr. Briggs is a graduate of the University of Tennessee at Chattanooga with a bachelor's degree in Computer Science Information Security and Assurance and also majoring in Software Applications. He holds the following certifications: SANS Global Information Assurance Certification (GIAC) Response and Industrial Defense (GRID), CISSP, Certified Authorization Professional, and Software Engineering Institute Computer Emergency Response Team (CERT)-Certified Computer Security Incident Handler. Prior to entering into the cyber security field, Mr. Briggs was a sergeant in U.S. Army 2-14 Infantry Regiment 10th Mountain Division.

Stuart Brindley
President
S. J. Brindley Consulting Inc.

Stuart Brindley is a registered Professional Engineer with more than 35 years of experience in the electricity industry in diverse roles that include power system operations, information security, customer billing, and distribution. In 2010, Mr. Brindley retired from the Independent Electricity System Operator in Ontario, Canada, where, among other responsibilities, he led Ontario's Electricity Emergency Management program. He has since been providing professional services to the electricity industry, trade associations, regulators, and government.

Over the past decade, Mr. Brindley has helped lead the development of the electricity industry's CIP program across North America. He is the founding chair of the CEA's critical infrastructure program, past chair of NERC's CIPC, and past chair of the U.S. Partnership for Critical Infrastructure Security.

Michael Chaffee
Director, Sales, Security
FLIR Systems, Inc.

Michael Chaffee is a 20-year veteran of FLIR Systems Inc., and as part of the FLIR security team, has participated in many monumental innovations in the world of thermal imaging for perimeter security. Mr. Chaffee has witnessed the growth in utilization of FLIR technology across many critical infrastructure verticals.

Well-versed in thermal cameras married to analytics and its best practices, Chaffee's core expertise centers around utility perimeter substation projects, where he has guided many complex solutions. Mr. Chaffee has a bachelor's degree in Broadcast Communications from the University of Wisconsin.

Sam Chanoski
Director, Intelligence
E-ISAC

Sam Chanoski is the E-ISAC's director of Intelligence, where he works with government and private sector organizations to share all-source intelligence in the context of the electricity industry, develop mitigation strategies for significant grid threats, and provide technical and business context to the E-ISAC's activities.

Before joining the E-ISAC, Mr. Chanoski led NERC's Bulk Power System Awareness and Event Analysis teams. Prior to coming to NERC, he worked for several years with investor-owned utilities in real-time operations and maintenance roles.

Mr. Chanoski's academic background is in computer science and operations research with a graduate degrees in Business, Engineering, and Information Security as a complement to more than 15 years of military reserve service, where he provided intelligence support to defensive cyber operations. His professional interests include real-time transmission and distribution operations, organizational behavior, control systems cyber security, and emergency management and resilience.

Tim Conway
Technical Director, ICS and SCADA Programs
SANS

Tim Conway serves as the technical director, ICS and SCADA programs at SANS, and is responsible for developing, reviewing, and implementing technical components of the SANS ICS and SCADA product offerings. Additionally, he performs contract and consulting work in the areas of ICS cyber security with a focus on energy environments.

A recognized leader in CIP operations, Mr. Conway formerly served as the director of CIP Compliance and Operations Technology at Northern Indiana Public Service Company (NIPSCO), and was responsible for OT, NERC CIP Compliance, and the NERC training environments for the operations departments within NIPSCO Electric.

Recognizing the need for ICS-focused cyber security training throughout critical infrastructure environments and an increased need for NERC CIP hands-on training, Mr. Conway authored and instructs the ICS curriculums newest course ICS456 - Essentials for NERC Critical Infrastructure Protection.

Outside of SANS, Mr. Conway continues to perform contract and consulting work in the areas of ICS cyber security with a focus on the energy sector.

Dustin Cornelius
End Point Security Principal
Southern Company

Dustin Cornelius is an end-point security principal for Southern Company Transmission Energy Management System. Mr. Cornelius has 23 years of experience in IT and network security with the last 10 years focused on network- and host-based security for ICS. He is the Southern Company lead planner for GridEx and has successfully planned and executed GridEx III and GridEx IV for Southern Company as a part of the North American electricity industry incident response tabletop. He also serves as the cyber team lead for the NERC GEWG. Mr. Cornelius earned a master's degree in Engineering from the University of Alabama at Birmingham and a CISSP.

Matthew Duncan
Manager, Policy and Coordination
E-ISAC

Matthew Duncan serves as the policy and coordination manager at the E-ISAC, focusing on North American electricity industry resilience policy and cross-sector coordination. Previously, Mr. Duncan was a program manager at the U.S. DOE, managing sector-specific agency and state government outreach. Mr. Duncan has also served as deputy U.S. political officer at the Helmand Provincial Reconstruction Team in Afghanistan, a strategic policy analyst for the U.S. Department of Defense (DOD), and a research assistant for the Offices of the United States Attorneys in the U.S. Department of Justice (DOJ).

Mr. Duncan earned a GIAC Global Critical Infrastructure Protection Certificate, a bachelor's degree from Saint Joseph's University, and a master's degree in International Relations from the Maxwell School of Citizenship and Public Affairs at Syracuse University.

Karen S. Evans
Assistant Secretary, CESER
U.S. DOE

Karen S. Evans was sworn in by U.S. Deputy Secretary of Energy Dan Brouillette as the assistant secretary for CESER on September 4, 2018. Before being nominated by President Trump to lead the U.S. DOE's cyber security efforts, Mrs. Evans served in the public sector as a top IT official at the U.S. Office of Management and Budget under President George W. Bush in the position that is now known as the federal chief information officer (CIO). She has also previously served as the U.S. DOE's CIO. Most recently, Mrs. Evans was the national director of the U.S. Cyber Challenge, a public–private program designed to help address a skills gap in the cyber security field.

Mrs. Evans received a bachelor's degree in Chemistry and a master's degree in Business Administration from West Virginia University.

Tami B. Fowler
Senior Program Manager, Emergency Preparedness
TVA

Tami Fowler serves as the senior program manager for Emergency Preparedness for TVA. Ms. Fowler is responsible for providing technical direction, support, and oversight for TVA's nonradiological Emergency Preparedness Programs. She is responsible for maintenance and operability of corporate emergency systems, ensuring readiness of emergency facilities, tools, and resources through corporate-level training and exercise scenarios.

Ms. Fowler earned master's degrees in Emergency Planning and Disaster Management and Public Administration with a concentration in Environmental Policy, both from American Military University. She also earned a Certified Emergency Manager designation from the International Association of Emergency Managers and is a member of the Emergency Management Association of Tennessee.

David Godfrey
Critical Infrastructure Protection Manager
GP&L

David Godfrey is responsible for ensuring compliance of the Critical Infrastructure Protection Standards for GP&L and Texas Municipal Power Agency (TMPA). He also manages all aspects of GP&L's physical security and the physical security of TMPA's transmission assets. He previously served as security and facilities manager for TMPA.

Mr. Godfrey has 29 years of experience in the electric utility industry. He is an original and active member the E-ISAC Physical Security Advisory Group (PSAG), a contributor to the *Electricity Sector Design Basis Threat* reference document, a participant in several DBT implementation exercises, and an active member of the Electric Reliability Council of Texas (ERCOT) Critical Infrastructure Protection Working Group. He attended Sam Houston University and has a State of Texas Master Peace Officer certification.

Howard Gugel
Vice President and Director, Engineering and Standards
NERC

Howard Gugel is the vice president and director of Engineering and Standards at NERC. In this role, he is responsible for providing engineering analysis and support for NERC activities and directing all aspects of NERC's continent-wide standards development process by providing oversight, guidance, coordination, and industry education of the development of Reliability Standards. Mr. Gugel previously served as the director of Performance Analysis, where he was responsible for the development, maintenance, and analysis of reliability performance metrics, including those in NERC's annual *State of Reliability* report. This included analyzing various databases of transmission and generations outages to look for statistically significant trends. Mr. Gugel has more than 29 years of experience in the electric utility industry.

Prior to joining NERC, Mr. Gugel was a transmission area maintenance manager for Progress Energy Florida, where he managed a staff of field personnel who maintained transmission lines and substation equipment. Prior to that, he was a transmission planning manager, also for Progress Energy Florida. Mr. Gugel's background includes management experience in operations and energy marketing. He has worked for two investor-owned utilities, a rural electric co-op, and an energy marketing firm.

Mr. Gugel earned his bachelor's and master's degrees in Electrical Engineering from the University of Missouri – Rolla. He is a licensed Professional Engineer in Missouri.

Brian Harrell
Assistant Director, Infrastructure Security Division, CISA
U.S. DHS

In December 2018, President Trump appointed Brian Harrell to serve as the U.S. DHS's assistant secretary for Infrastructure Protection. Mr. Harrell now serves as the first assistant director for Infrastructure Security within CISA. Recently recognized as one of Security Magazine's Most Influential People in Security, Mr. Harrell is the former managing director of Enterprise Security at the Duke Energy Corporation. He is also the former director of the E-ISAC and director of CIP programs at NERC. Mr. Harrell has spent time during his career in the U.S. Marine Corps and various private sector agencies with the goal of protecting the United States from security threats.

Kurt Hoffmann
Information Security Program Adviser
Berkshire Hathaway Energy

Kurt Hoffman serves as an information security program adviser at Berkshire Hathaway Energy. He manages the Berkshire Hathaway Energy Cyber Threat Intelligence program, which supports critical infrastructure security operations centers on three continents and more than 12 million direct customers. His past experience includes leading the threat intelligence programs at MidAmerican Energy as well as reinventing the IT disaster recovery process at MidAmerican Energy.

Mr. Hoffman's security engagement concentrates on global events and the preventative measures that can be taken at the local level to reduce and mitigate impacts. He has assisted in developing and executing multiple energy sector-specific exercises at both the local and national level, including GridEx III and GridEx IV, Iowa's 2016 public–private Coordinated Electric Exercise, and other industry-specific simulations. Mr. Hoffman also served in a planning and player role in the first exercise of the Electricity Subsector Coordinating Council's (ESCC) Cyber Mutual Assistance program. Mr. Hoffman has multiple cyber security certifications, including the CISSP, GIAC Cyber Security Essentials, and the GIAC Cyber Threat Intelligence (GCTI).

Jason Ivall
Program Manager, Infrastructure Protection and Security
CEATI International

Jason Ivall is a program lead at CEATI International, where he manages four utility interest groups: Strategic Options for Integrating Emerging Technologies and Distributed Energy Interest Group, Infrastructure Protection and Security Interest Group, Thermal Generation Interest Group, and Demand Side Energy Management Program.

Mr. Ivall earned a master's in Engineering and doctorate in Chemical Engineering at McGill University, where he led cross-disciplinary projects on the use of nanomaterials and natural gas hydrates for carbon dioxide capture and sequestration as well as for phase-change materials for energy storage. He subsequently served as the course lecturer for a fourth-year Energy Systems Engineering course. With a strong background in energy science and innovation, Mr. Ivall applies a research mindset to understand the challenges of the electricity industry, curate program initiatives that support member needs, and advance the sector through collaboration.

David Jarrett
Senior Advisor, Physical Security
SCE

David Jarrett has 38 years of law enforcement and security experience, consisting of local law enforcement, security consulting, licensed private investigator, and qualified manager for a security company. Mr. Jarrett is a senior advisor in Physical Security for SCE and has conducted risk, vulnerability, and threat assessments for external clients and currently for internal clients. He is responsible for reviewing physical security mitigation requests and aligns them with strategic plans, current standards, guidelines, and best practices.

Mr. Jarrett holds several certifications through ASIS International including Certified Protection Professional, Professional Certified Investigator, and Physical Security Professional. He is a member of ASIS International and its Utility Security Council, the Association of Threat Assessment Professionals, International Crime Prevention Through Environmental Design Association, and the Police Officers Research Association of California. Mr. Jarrett holds a bachelor's degree in Criminal Justice Management.

Ross Johnson
President
Bridgehead Security Consulting, Inc.

Ross Johnson is the president of Bridgehead Security Consulting, Inc. Mr. Johnson served in the Canadian Forces as an infantry and intelligence officer for 24 years. Since leaving the service in 2001, Mr. Johnson has been employed in several security-related leadership positions in aviation security, the offshore oil industry, and the electricity industry. Mr. Johnson was responsible for physical and cyber security as the director of Security and Contingency Planning with EPCOR Utilities, and he joined Capital Power as the senior manager of Security and Contingency Planning in 2009. He remained at Capital Power until leaving to create Bridgehead Security Consulting in 2019.

Mr. Johnson is an infrastructure security advisor for Awz Ventures, a North American hub for cutting-edge cyber security, intelligence, and physical security technologies and solutions from Israel—a global leader in these sectors. He has also been a long-time participant with NERC, serving as a member of CIPC and as the physical security lead on the Executive Committee. He is currently the co-chair of the E-ISAC's PSAG. In addition, Mr. Johnson is the chair of the Provincial Electricity Sector Physical Security Working Group in Alberta, which promotes public safety, the resilience of critical infrastructure, and crime prevention. He is a past chair of CEA's Security and Infrastructure Protection Committee (SIPC) and is a council vice president at ASIS International. He is a member of Natural Resources Canada's Energy and Utilities Sector Network and the author of *Antiterrorism Planning and Threat Response*, a book on the prevention of terrorist attacks.

Mr. Johnson has a bachelor's degree in Military Arts and Sciences with distinction from the Royal Military College of Canada and is board-certified in Security Management by ASIS International.

Jeff Jones
Manager, Industrial Cyber Security
E-ISAC

Jeff Jones is the manager of Industrial Cyber Security at the E-ISAC. He is passionate about securing our nation's critical infrastructures. He has spent more than 16 years in information security and cyber risk management with particular expertise in industrial control and SCADA system cyber security. Mr. Jones spent 13 of those years at one of the nation's largest electricity providers, holding different positions in its industry-leading cyber security organization.

Mr. Jones joined the E-ISAC in 2017, and he enjoys expanding capabilities through building relationships, strategizing, and creating threat intelligence specific to the electricity industry to provide worldclass, trusted, quality analysis to help reduce cyber security risk to critical infrastructures. Mr. Jones helped beta-test the Global Industrial Cyber Security Professional certification and was one of the first 50 individuals to earn it. Other certifications he maintains include the following: CISSP, Certified Information Security Manager (CISM), GCTI, and GRID.

Kathy Judge
Head of U.S. Physical Security
National Grid

Kathy Judge is head of U.S. Physical Security for National Grid. Ms. Judge is responsible for managing National Grid's strategies and best practices required to protect energy delivery facilities in accordance with governing security regulations in the United States. Ms. Judge has 31 years of service with National Grid.

Ms. Judge is actively engaged with state and federal agencies to help shape security policies and procedures. She currently serves as chair of the Pipeline Sector Coordinating Council, co-chair of the Northeast Power Coordinating Council's Physical Security Committee, and as a member of the ONG SCC. In addition to her extensive engagement with government agencies, she is past chair of AGA's Security Committee.

Ms. Judge has a master's degree in Business Administration from Nichols College.

Jake Kouns
CISO and COO
Risk Based Security

Jake Kouns co-founded Risk Based Security, a company that provides the world's leading vulnerability and data breach intelligence and vendor risk ratings to clients, many of whom are critical energy providers. Mr. Kouns previously oversaw the operations of the Open-Sourced Vulnerability Database (OSVDB.org) and DataLossDB. He has worked as the director of Cyber Security and Technology Risks Underwriting for Markel and managed network security for Capital One.

Mr. Kouns has briefed the U.S. DHS and U.S. DOD on cyber liability insurance issues and is frequently interviewed as an expert in the security industry. He is the founder of RVAsec and has presented at many well-known security conferences, including RSA, Black Hat, and DEF CON. Mr. Kouns is the co-author of *Information Technology Risk Management in Enterprise Environments* and *The Chief Information Security Officer*. He has a bachelor's and master's degree in Business Administration with a concentration in Information Security from James Madison University. Mr. Kouns also has several certifications, including ISC2's CISSP, ISACA's CISM, CISA, and Certified in the Governance of Enterprise IT.

Tamara Lance
Director, Information Security
Atmos Energy Corporation

Tamara Lance is the director of Information Security at Atmos Energy Corporation and has more than 20 years of experience in the field of IT. In her current role, Ms. Lance provides day-to-day leadership, strategic planning, and the long-term vision for Atmos Energy's Information Security program. Ms. Lance has extensive experience in hardware and software development as well as infrastructure management. Prior to joining Atmos Energy, she held multiple leadership roles at Dell Incorporated within the hardware development and IT organizations.

Ms. Lance is the chair of the ONG SCC, which works with the U.S. DOE, U.S. DHS, and other governmental agencies on sector-specific security strategies and provides communication across the sector. She is on the Board of Directors for the DNG-ISAC and is an active member of AGA's Security Committee and Cybersecurity Strategy Task Force.

Bill Lawrence
Vice President and CSO
NERC

As NERC's vice president and CSO, Bill Lawrence is responsible for the oversight of the E-ISAC and for directing security risk assessment and mitigation initiatives to protect critical electricity infrastructure across North America. He also leads coordination efforts with government agencies and stakeholders on cyber and physical security matters, including analysis, response, and sharing of critical sector information. Prior to his role as CSO, Mr. Lawrence managed and grew programs such as GridEx and GridSecCon.

Prior to joining NERC, Mr. Lawrence had a distinguished career in the U.S. Navy, where he served as a pilot of F-14 Tomcats and F/A-18F Super Hornets. He also served as the deputy director in the Character Development and Training Division at the U.S. Naval Academy, where he taught courses in Ethics and Cyber Security. In 2012, after more than 20 years of faithful service, Commander Lawrence honorably retired from the U.S. Navy. His awards include four Air Medals, three Navy Commendation Medals, and various unit and campaign awards.

Lawrence has a bachelor's degree in Computer Science from the U.S. Naval Academy, a master's degree in International Relations from Auburn Montgomery, and a master's degree in Military Operational Art and Science from the Air Command and Staff College. He also earned a Project Management Professional (PMP) certification and several cyber security certifications.

François Lemay
Cyber Security Specialist
Hydro-Québec

François Lemay is a cyber security specialist at the Cyber Security Operation Center at HydroQuébec, where he has been a part of the cyber security unit for the last 14 years. Mr. Lemay is an active member on CEA's SIPC, learning the essentials of industry's security posture and threat environment.

Prior to his current role, Mr. Lemay held other positions focused on IT and cyber security in utilities and other industries. He has a CISSP and CISA and is passionate about security, looking for new threats, and correlations with geopolitical issues.

Suzanne Lemieux
Manager, Midstream and Industry Operations
API

Suzanne Lemieux has been with API since 2013 and serves as a manager within the Midstream and Industry Operations unit. Her primary areas of responsibility are emergency preparedness and response, security policy, maritime policy, UAS policy, energy infrastructure advocacy, and public and private stakeholder engagement. Ms. Lemieux previously worked for BCS Incorporated as the manager of the Emergency Response and Risk Management team and as a senior analyst in the U.S. DOE's Office of Electricity Delivery and Energy Reliability. Ms. Lemieux supported the U.S. DOE's efforts to build public–private partnerships with the oil and natural gas and electricity sectors.

Ms. Lemieux is a certified PMP and is a graduate of Harvard University's National Preparedness Leadership Initiative Executive Education. She has a bachelor's degree in Business Administration focused on Marketing Management from Radford University and a master's degree in Public and International Affairs from the Virginia Polytechnic Institute and State University.

Ben Miller
Vice President, Professional Services and R&D
Dragos

Ben Miller is vice president of Professional Services and R&D at the industrial cyber security company Dragos, Inc., where he leads a team of analysts in performing active defense inside of ICS/SCADA networks. In this capacity, Mr. Miller is responsible for a range of services including threat hunting, incident response, penetration testing, and assessments for the industrial community as well as advanced research and innovation within ICS security.

Mr. Miller was previously an associate director at the E-ISAC and led cyber analysis for the industry. He and his team focused on leading-edge cyber activities as they related to the North American BPS. Mr. Miller served in both planner and player roles in GridEx I, II, and III. He served as a facilitator of several NERC task forces, including the Cyber Attack Task Force and is an acknowledged contributor to National Institute of Standards and Technology Special Publication 800-150. Mr. Miller was recognized as instrumental in building new capabilities surrounding information sharing and analytics during his five years at the EISAC.

Prior to joining the E-ISAC, Mr. Miller built and led a team of nine people, focused on network security monitoring, forensics, and incident response, at a Fortune 150 energy firm. His team received numerous accolades from industry and law enforcement. Mr. Miller is an accomplished speaker in various venues, including Black Hat, SANS, the Industrial Control Systems Joint Working Group, ShmooCon, and others. He was recognized by SANS as a 2017 Difference Maker Award winner for his contributions to the electricity industry.

Nathan Mitchell
Senior Director, Cyber and Physical Security Services
APPA

Nathan Mitchell is the senior director of Cyber and Physical Security Services for APPA. Mr. Mitchell provides leadership in cyber and physical security issues for APPA members and is the principal investigator of a three-year program using U.S. DOE funds to develop cyber security tools, educational resources, guidelines, and training on strategies that public power utilities can use to address cyber risk.

Prior to joining APPA in 2006, he served for 10 years at the City of Naperville, Illinois, in the Department of Public Utilities, where he was the electric distribution manager in charge of utility operations and construction. Mr. Mitchell has a bachelor's degree in Electrical Engineering from Iowa State University and is a registered Professional Engineer in Illinois.

Travis Moran
Vice President, Operations
Welund North America

Travis Moran is a retired law enforcement professional with more than 26 years of enforcement, security, and intelligence experience. He is currently the vice president of Operations for Welund North America.

Mr. Moran began his federal law enforcement career with the U.S. National Central Bureau Interpol before transitioning to the U.S. Department of State and then ultimately the U.S. DOJ, Bureau of Alcohol, Tobacco, Firearms, and Explosives, where he spent his last 15 years.

Mr. Moran has extensive experience in energy security, where he worked as a physical security specialist for both investor-owned utilities and NERC. He has become an energy-specific subject matter expert regarding threats posed to energy companies from activism and UAS.

Mr. Moran has a master's degree in Criminology, Law, and Society, and a master's degree in Criminology.

Bill Peterson
Manager, Entity Outreach and Training
SERC

Bill Peterson is the manager of Entity Outreach and Training with SERC, a corporation responsible for promoting and improving the reliability, adequacy, and critical infrastructure protection of the BPS in all or portions of 16 southeastern and central states.

Previously, Mr. Peterson was the program manager of Cyber Security in the Technical Resources department leading the SERC CIPC in all initiatives. He also served as a senior CIP engineer in the Compliance group leading audits and risk mitigation efforts for assigned entities. Prior to joining SERC, he was a CIP lead with Duke Energy working on various CIP projects, audit preparations, mitigation plans, and self-reports. Mr. Peterson was also a CIP analyst and system administrator with the New York Power Authority working on CIP audit preparations, system administration, network security, network operations, and IT project management.

Mr. Peterson has a bachelor's degree with a dual major in Computer Engineering and Electrical Engineering Technology from the State University of New York at Utica/Rome. He also has a master's degree in Business Administration with a concentration on Information Technology Management from the State University of New York at Utica/Rome. In addition, Mr. Peterson's certifications include the following: CISM, CISSP, Certified in Risk and Information Systems Control, and a leadership certificate from Cornell University.

James B. Robb
President and CEO
NERC

James B. Robb assumed the role of president and CEO of NERC in April 2018. Mr. Robb oversees NERC's mission of assuring the reliability and security of the North American BPS. As president and CEO, Mr. Robb directs key programs affecting more than 1,400 BPS owners, operators, and users, including mandatory NERC Reliability Standards, compliance monitoring, enforcement, situational awareness, event and risk analysis, reliability assessments and forecasting, cyber and physical security, and government relations. Mr. Robb also oversees the operations of the Regional Entities who support the reliability mission across North America.

From 2014 to 2018, Mr. Robb served as president and CEO of the Western Electricity Coordinating Council (WECC), where he was responsible for the strategic direction and leadership of all of WECC's activities.

Mr. Robb has more than 30 years of experience in the energy sector as an engineer, a consultant, and a senior executive. Prior to becoming WECC's CEO in 2014, he held three major leadership roles in the industry at Northeast Utilities (now Eversource Energy) as senior vice president of Enterprise Planning and Development, at Reliant Energy (now part of NRG Energy) as senior vice president of Retail Marketing for the competitive retail business in Texas and the Northeast, and at McKinsey & Company as a partner and leader of the West Coast's Energy and Natural Resource Practice. During his 15-year career at McKinsey, he worked closely with prominent electric power companies in California, Western Canada, the Pacific Northwest, and the Rocky Mountain states as well as with some of the region's largest energy consumers.

Mr. Robb earned a bachelor's degree in Chemical Engineering from Purdue University and a master's degree in Business Administration from the Wharton School of Business at the University of Pennsylvania.

Sam Rozenberg
Engineering Services Security Director
APPA

Sam Rozenberg joined APPA in December 2016 and is the engineering services security director at APPA. He has worked with utilities on a variety of physical and cyber security issues as well as emergency response.

Before joining APPA, Mr. Rozenberg worked for Progress Energy and later Duke Energy for 6 years, overseeing physical security operations for 32 hydro stations in 3 states as well as a 24/7 Global Security Operations Center.

Mr. Rozenberg earned his bachelor's degree in International Criminal Justice and his master's degree in Public Administration degree from John Jay College of Criminal Justice in New York City and completed the Security Executive Council's Next Generation Security Leadership Program.

David Rudawitz
Critical Infrastructure Advisor
NVIS Communications

David Rudawitz is the critical infrastructure advisor to NVIS Communications. At NVIS, Mr. Rudawitz works with electricity and other critical infrastructure sector entities to develop, deploy, and maintain resilient communications systems to support emergency, disaster, and cyber security operations.

Prior to joining NVIS, Mr. Rudawitz was a contract project manager and subject matter expert at the Bonneville Power Administration where he developed and deployed a high-frequency emergency communication system and emergency response plans and exercises for all hazards, including cyber incidents. Mr. Rudawitz has more than 45 years of experience in emergency communications and disaster incident management and response. He has worked in the electricity industry since 2008, developing incident response plans and resilient communications systems built on a core of high-frequency radio equipment. His work has also supported the development of cyber incident response plans and the application of the FEMA Incident Command System for the management of these incidents. Mr. Rudawitz is also a certified project manager.

Laura Marshall Schepis
Senior Director, National Security
EEI

Laura Marshall Schepis is senior director of National Security for EEI, where she leads EEI's participation in and support of the ESCC. After passage of the 2005 Energy Policy Act put new mandatory standards in place for many energy companies, Ms. Schepis created NRECA's legislative grid security practice, fostered creation of the electric utility grid security coalition, and helped stand up the initial ESCC.

Across 19 years of federal and state advocacy, Ms. Schepis has directed lobbying efforts on telecommunications, appropriations, commodity trading, natural gas regulation, energy efficiency, and renewable energy standards. She also designed and led significant political campaigns on climate change, solar energy, and retail competition, and ran one of the largest national energy political action committees.

Ms. Schepis is a graduate of the University of Georgia School of Law and practiced civil and criminal law in Georgia before relocating to Washington, D.C., in 2000.

Jake Schmitter
Senior Manager, Training and Exercises
E-ISAC

Jake Schmitter is the senior manager for Training and Exercises at the E-ISAC. He is the exercise lead for GridEx—a biennial training exercise that is focused on government and industry response to and recovery from the consequences of a coordinated cyber and physical threat to the North American electrical grid.

Prior to joining the E-ISAC, Mr. Schmitter was the lead planner for U.S. Cyber Command's CYBER GUARD exercise—a defensive cyber training event focused on domestic responses to cyber attacks against critical infrastructure. He is a former naval aviator with more than 21 years in the U.S. Navy.

Mr. Schmitter earned his bachelor's degree from the U.S. Naval Academy and his master's degree from the Naval Postgraduate School. He is a commander in the Navy Reserve.

Carter Schoenberg
Executive Vice President, Cybersecurity Solutions
IPKeys Power Partners

Carter Schoenberg is the executive vice president of Cybersecurity Solutions with IPKeys Power Partners and is a cyber and privacy risk subject matter expert supporting government and commercial markets to better define how cyber, legal, and insurance matters converge and impact organizations.

Mr. Schoenberg is a CISSP with more than 25 years of combined experience in criminal investigations, cyber threat intelligence, cyber security, risk management, and cyber law. His work products have been actively used by the U.S. DHS and U.S. DOD, the ISAC communities, and the Georgia Bar Association for Continuing Legal Education credits on the topic of cyber security risk and liability. Mr. Schoenberg's expertise is profiled at conferences, including the following: National Association of Insurance Commissioners Annual Conference, Council for Insurance Agents and Brokers, ISC2, SecureWorld Expo, Information Systems Security Association, Latin American Insurance and Reinsurance Forum, and InfosecWorld.

Ray Sefchik
Director, Reliability Assurance
ReliabilityFirst

Ray Sefchik is the director of Reliability Assurance at ReliabilityFirst. He leads the Risk Analysis and Mitigation team as well as the Entity Development team. In previous roles at ReliabilityFirst, Mr. Sefchik led the Events Analysis and Situational Awareness team and the CIP Compliance Monitoring team. Mr. Sefchik is an experienced information security, audit, risk, and compliance professional. He has the CISA, CISM, and CISSP security certifications.

Hailey Siple
Manager, National Security Policy
EEI

Hailey Siple serves as senior analyst National Security Policy at EEI and supports the ESCC. Ms. Siple is the secretariat lead for the ESCC R&D Strategic Committee, where she drives industry-wide R&D efforts to identify and enhance mitigation strategies for threats to the operation and security of the electric grid with a focus on enhancing public–private R&D partnerships.

Prior to joining EEI, Ms. Siple supported Federal Government Affairs at Teva Pharmaceuticals. She received her bachelor's and master's degrees in Philosophy from the University of Houston.

Brian Thumm
Vice President, Performance Improvement and Risk Mitigation
SERC

Brian Thumm is the vice president of Performance Improvement and Risk Mitigation, leading SERC's risk assessment and mitigation, training and outreach, and strategic initiatives and continuous improvement departments. The combination of these roles provides a unique platform from which to communicate emerging and persistent risks to a broad stakeholder base and to work with registered entities to resolve those risks in a collaborative manner.

Mr. Thumm is also responsible for several internal oversight functions, including quality assurance, internal controls, program readiness, operational excellence, continuous improvement, and the Project Management Office.

Prior to joining SERC, Mr. Thumm served as director of Regional Planning for ITC Holdings Corp. There, he led a group of engineers engaged in economic planning analysis, load forecasting, stability analysis, technical studies, and NERC compliance as well as ITC's post-Order 1000 planning-related efforts across the country. Mr. Thumm has more than 25 years of electric industry experience, including holding positions in transmission planning, transmission operations, regulatory strategy, external affairs, project development, nuclear licensing, and computer services.

Mr. Thumm received a bachelor's degree in Electrical Engineering from Rensselaer Polytechnic Institute, a master's degree in Business Administration from Michigan State University, and a master's degree in Electrical Engineering from Tulane University. He is a registered Professional Engineer in Michigan and Louisiana and a certified PMP.

Zach Tudor
Associate Laboratory Director, National and Homeland Security
INL

Zach Tudor is the associate laboratory director of INL's National and Homeland Security (N&HS) directorate—a major center for national security technology development and demonstration, employing 550 scientists and engineers across $300M in programs for the U.S. DOD, U.S. DHS, and the intelligence community. N&HS is responsible for INL's Nuclear Nonproliferation, Critical Infrastructure Protection, Defense Systems, and Homeland Security missions, including safeguarding and securing vulnerable nuclear material, enhancing the overall security and resilience of the nation's infrastructure, and providing protective system solutions and heavy manufacturing of armor for national defense.

Mr. Tudor has more than 30 years of experience in IT and cyber security management, operations, and incident response. Past positions include program director in the computer science laboratory at SRI International, support to the Control Systems Security Program and the ICS-CERT at the U.S. DHS, onsite deputy program manager for the National Reconnaissance Office's world-wide operational network, information security manager for the Office of the Secretary of Defense CIO's Enterprise Operations Support Team, and security management support for the Centers for Medicare and Medicaid Services. Mr. Tudor has a master's degree in Information Systems with a concentration in Cyber Security from George Mason University.

Matt Wakefield
Director, Information and Communications Technology R&D
EPRI

Matt Wakefield is a director of Information and Communications Technology R&D at EPRI. His responsibilities include furthering the development of a modernized grid with a strong focus on leveraging emerging information and communication technologies that can be applied to the electric grid infrastructure. Mr. Wakefield manages EPRI's Smart Grid Research focused on enabling advanced applications, including the IntelliGrid Program, Cyber Security and Privacy Program, and multi-year international Smart Grid Demonstration initiative.

Mr. Wakefield started his career in 1986 in the U.S. Navy, serving as a nuclear power plant reactor operator and engineering supervisor in the submarine feet and specializing in electronic instrumentation and controls.

Mr. Wakefield then joined Wisconsin Public Service Corp. (WPS) in the Instrumentation and Control Group of the Kewaunee Nuclear Plant before becoming manager of the Applied Technology group at Integrys Energy Group, the holding company of WPS. At Integrys, Mr. Wakefield focused on developing and applying information and communication technologies related to low-cost, real-time, energy-related information transfer between control centers, generators, markets, and consumers. This team developed a number of innovative solutions, including DENet and eMiner that used emerging open-source software and low-cost embedded hardware while leveraging the Internet for a virtually free communication infrastructure.

Tabice Ward
Director, Information Protection and Security, CISO
DTE Energy

Tabice Ward is director of Information Protection and Security at DTE Energy, a Detroit-based diversified energy company involved in the development and management of energy-related businesses and services nationwide. DTE Energy's operating units include an electric utility serving 2.1 million customers in southeastern Michigan and a natural gas utility serving 1.2 million customers in Michigan. The DTE Energy portfolio also includes non-utility energy businesses focused on power and industrial projects, natural gas pipelines, gathering and storage, and energy marketing and trading.

Ms. Ward is responsible for overseeing DTE Energy's cyber security program and compliance, which includes network and application security, identity access management, security operations center, security awareness, cyber risk management, security standards, and business continuity and crisis response planning for IT. Additionally, her responsibilities include representing DTE Energy across multiple externally facing industry groups, committees, and forums (such as EEI, AGA, Interstate Natural Gas Association of America, and UNITE) that support CIP.

Dave Whitehead
COO
SEL

Dave Whitehead is COO at SEL. After joining SEL in 1994, Mr. Whitehead served in a variety of roles within the company, including hardware engineer, research engineer, chief engineer of the Government Services Division, and vice president of R&D.

A passionate driver of product and talent development at SEL, Mr. Whitehead has had a hand in the steady stream of inventions and innovations to come out of the U.S.-based technology company. He has been awarded more than 60 patents around the world.

Mr. Whitehead is a leader in utility and ICS cyber security. He has presented at conferences, testified before FERC, chairs the IEEE Power and Energy Society Substations C6 group that addresses serial cryptographic protocols, and has authored numerous papers on the topic.

Mr. Whitehead received his bachelor's degree in Electrical Engineering from Washington State University and his master's degree in Electrical Engineering from Rensselaer Polytechnic Institute. He is a registered Professional Engineer in Washington, New York, Michigan, and North Carolina.

Ginger Wright
Energy-Cyber Portfolio Manager, Cybercore
INL

Ginger Wright is the energy-cyber portfolio manager for INL's Cybercore division within its N&HS directorate. She leads programs focused on cyber security and resilience of critical infrastructure for the U.S. DOE, the Defense Advanced Research Projects Agency (DARPA), and other government agencies including U.S. DOE's Cyber Analytics Tools and Techniques, Cyber Security for the Operational Technology Environment, and Cyber Testing for Resilience of the Industrial Control Systems.

Ms. Wright has a significant technical and program management background through her work at the laboratory, in government, education, and private organizations. She focuses on designing and managing research projects to improve cyber security and cyber restoration of critical infrastructure systems, including the power grid and nuclear facilities. Ms. Wright is renowned for her ability to create collaborative, multidisciplinary environments for researchers. Her work on cyber-informed engineering and her research in component analysis for critical infrastructure digital assets are two recent impactful research efforts, gaining approval from the U.S. DOE, vendors, and asset owners.

Ms. Wright has held various positions at INL, including domestic nuclear cyber security program manager, conduct of research lead for INL chief research officer, deputy director and projects manager for mission support center, and principle investigator for the INL team for DARPA National Cyber Range. Prior to joining INL, she was a project manager at the Central Intelligence Agency.

Ms. Wright has a bachelor's degree in Information Systems and Operations Management from the University of North Carolina at Greensboro.

Kristen Worosz
Senior Analyst
Welund

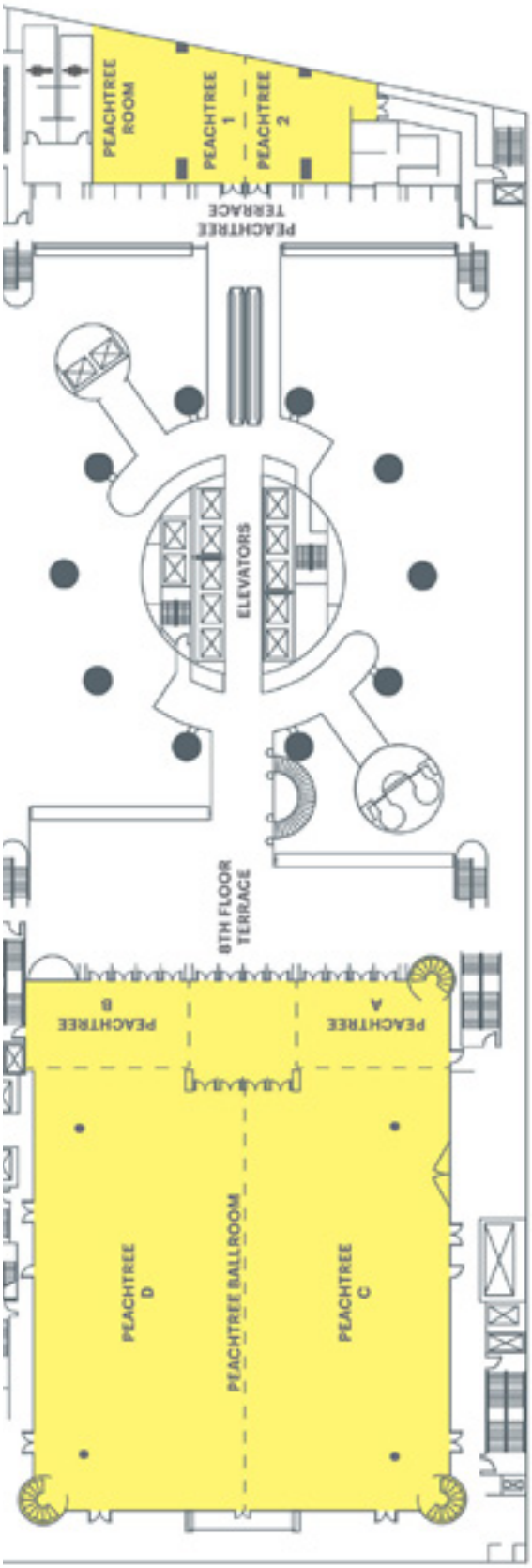
Kristen Worosz has more than 10 years of analytical experience in both the federal government and private sector. Ms. Worosz is currently a senior analyst at Welund, focusing on threats posed by activist groups, assessing their impact, and providing client-focused intelligence on risk management.

Prior to joining Welund, Ms. Worosz was the production manager at the E-ISAC, developing analytical products on the cyber and physical threats facing the electricity industry. Ms. Worosz also worked as a counterterrorism intelligence analyst for the U.S. FBI and as an analyst in the Investigations Division for the U.S. DOJ Office of the Inspector General.

Chastain Level, Sixth Floor

Augusta Level, Seventh Floor

Peachtree Level, Eighth Floor



Platinum Exhibitors

FORCE5 Inc

Booz | Allen | Hamilton

tripwire

CERTREC
YOUR REGULATORY EXPERTS

Gold Exhibitors

BURNS McDONNELL

Cooper Compliance

OWL
Cyber Defense

Exhibitors

CYBERGYM NYC

TOWERLINE SOFTWARE, LLC.

ARMORTEXT

ARCHER

IPKeys
POWER PARTNERS

cyrin

RSA

AVIGILON
a Motorola Solutions Company

IronNet

network perception

SEDC

xage
SECURITY

FLIR

CAST PERIMETER
LED SECURITY LIGHTING SOLUTIONS
1120-A Goffle Road Hawthorne, NJ 07506 cast-lighting.com 973.423.2303

VERVE
INDUSTRIAL PROTECTION

SOUTHWEST MICROWAVE

SpotterRF

ComplyTec
ENTERPRISE COMPLIANCE

ELECTRIC GUARD DOG

AMICO SECURITY

midwest
Security Products, Inc.
Solutions. Designed. Delivered.

CHAIN LINK FENCE MANUFACTURERS INSTITUTE

ConsoleWorks
Cybersecurity Operations Platform

RAZOR RIBBON
A PART OF Atkore INTERNATIONAL

SEL

FoxGuard Solutions
Cyber Security | Compliance | Industrial Computing

GATE SCANNER
Presented by BATELLE

RiskBased SECURITY

SENSTAR

doble

FORESCOUT

DRAGOS
SAFEGUARDING CIVILIZATION

GRESCO
TECHNOLOGY SOLUTIONS