GridSecCon 2018

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

WECC

October 16–19

Flamingo Las Vegas
3555 Las Vegas Boulevard South
Las Vegas, Nevada 89109

Contents

Welcome Letter

Welcome to our eighth annual grid security conference, GridSecCon 2018!

This year, the North American Electric Reliability Corporation (NERC) and the Western Electricity Coordinating Council (WECC) are jointly hosting the conference as part of the Electric Reliability Organization (ERO) Enterprise's efforts to protect the North American bulk power system through information sharing, education, and collaboration. GridSecCon represents the interaction among security professionals that we need to enhance our protection efforts as our interdependence grows.

Our work here focuses on the training, tools, and resources necessary for success in today's dynamic environment. NERC's Electricity Information Sharing and Analysis Center (E-ISAC) is essential to building a more complete picture of emerging threats and formulating effective mitigations and defenses to potential attacks. We must all effectively share actionable information and educate stakeholders about our efforts to strengthen the cyber and physical security of our grid.

This year, we have discussions led by organization leaders, including our co-hosts at WECC, the U.S. Department of Energy (DOE), Public Safety Canada, the U.S. Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the Electricity Subsector Coordinating Council, among others. These experienced experts will give you insights into the latest strategies and solutions to handle known and potential cyber and physical security threats.

Other topics include panel discussions on cross-sector and international information sharing, the current threat landscape, GridEx V planning, and game-changing research and development. 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.

The industry is innovative, but so are its opponents. Adversaries continue to develop more sophisticated campaigns that place the North American grid at risk, making events like GridSecCon increasingly important. Reliability and security are as interconnected as the workings of the grid itself; we cannot ensure reliability without also ensuring the security of the North American bulk power system. 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 (CEO)
NERC

Melanie Frye
President and CEO
WECC

Agenda

Monday, October 15, 2018 | Preconference

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

Twilight Foyer (Registration Desk)

Tuesday, October 16, 2018 | Training Day

7:30 a.m. **Registration**

Twilight Foyer

7:30–8:00 a.m. **Continental Breakfast**

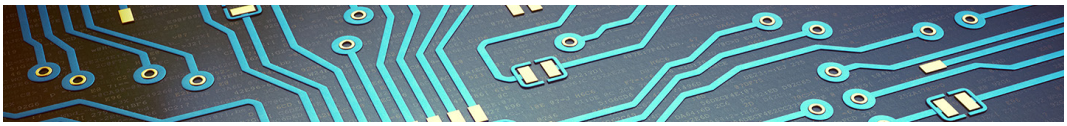
Twilight Ballroom

8:00 a.m.–Noon **Morning Sessions**

	Training Track	Training Provider	Location
1A	CyberStrike Workshop	DOE (Pick Both 1A and 1B)	Laughlin II (80 Seats)
2A	Physical Security Workshop I	E-ISAC Physical Security Partners	Laughlin I (60 Seats)
3A	Asset Management for Energy Providers	National Cybersecurity Center of Excellence (NCCoE) | National Institute of Standards and Technology (NIST)	Laughlin III (60 Seats)
4A	Build a Security Awareness Program Your Employees Will Love	Curricula, LLC	Reno II (40 Seats)
5A	Cybersecurity Training for SCADA using Testbed	Iowa State University	Virgina City I (24 Seats)
6A	Social Engineering and Open Source Intelligence Workshop	EC-Council	Virginia City II (95 Seats)

Noon–1:00 p.m. **Lunch**

Vista



1:00–5:00 p.m. **Afternoon Sessions**

	Training Track	Training Provider	Location
1B	CyberStrike Workshop	DOE (Pick Both 1A and 1B)	Laughlin II (80 Seats)
2B	Physical Security Workshop II	Pacific Northwest National Laboratory (PNNL)	Laughlin I (60 Seats)
3B	Next-Generation Cybersecurity for Electric Utility OT Networks	NCCoE | NIST	Laughlin III (50 Seats)
4B	How to be an Exercise Master Planner	Tennessee Valley Authority (TVA)	Reno II (40 Seats)
5B	Real-Time Threat Response	Tanium	Virgina City I (60 Seats)
6B	Who's in Your Network and How Long Have They Been There?	Burns & McDonnell	Virginia City II (95 Seats)

6:00–9:00 p.m. **Welcome and Networking Reception**

Exhibitor Hall (Twilight)

Wednesday, October 17, 2018 | Strategies and Threat Day

7:30–8:15 a.m. **Registration and Continental Breakfast**

Twilight Foyer and Ballroom

8:15–8:30 a.m. **Logistics**

Bill Lawrence, Vice President (VP) and Chief Security Officer (CSO), NERC; and Director, E-ISAC

Sunset/Vista Ballroom

8:30–8:45 a.m. **Trilateral Memorandum of Understanding Signing Ceremony**

Jim Robb, President and CEO, NERC

Katsuyuki Abe, Secretary General, Japan Electricity Information Sharing and Analysis Center (JE-ISAC)

Johan Rambi, Privacy and Cyber Security Advisor, European Energy-Information Sharing & Analysis Centre (EE-ISAC)

Sunset/Vista Ballroom

8:45–9:15 a.m. **Welcome Address and Opening Keynote**

Jim Robb, President and CEO, NERC

Sunset/Vista Ballroom

9:15–9:45 a.m.

Regional Entity Keynote

Melanie Frye, President and CEO, WECC

Sunset/Vista Ballroom

9:45–10:15 a.m.

Electricity Subsector Coordinating Council Strategy Keynote

Bill Fehrman, President and CEO, Berkshire Hathaway Energy

Sunset/Vista Ballroom

10:15–10:45 a.m.

Break

Twilight Ballroom

10:45–11:15 a.m.

Energy Keynote

The Honorable Karen Evans, Assistant Secretary, Office of Cybersecurity, Energy Security, and Emergency Response (CESER), DOE

Sunset/Vista

11:15–11:45 a.m.

E-ISAC Long-Term Strategic Plan

Bill Lawrence, VP and CSO, NERC; and Director, E-ISAC

Sunset/Vista Ballroom

11:45 a.m.–1:15 p.m.

Offsite Lunch

Bacchanal Buffet

Bacchanal walking instructions

1:15–1:45 p.m.

Homeland Security Keynote

Bob Kolasky, Director of the National Risk Management Center, National Protection and Progams Directorate (NPPD), DHS

Sunset/Vista Ballroom

1:45–2:15 p.m.

Law Enforcement and the Energy Sector

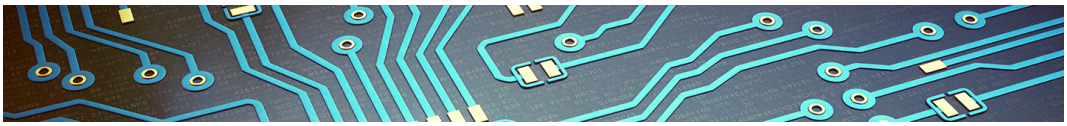
Michael Hickok, Assistant Special Agent in Charge, FBI Las Vegas

Sunset/Vista Ballroom

2:15–2:45 p.m.

Break

Twilight Ballroom



2:45–3:30 p.m.

Utilities Public–Private Partnership (P3) *(panel discussion)*

Moderator: G. David Brown, Jr., Lieutenant Colonel, Deputy Director of Domestic Operations for Planning, Training, and Exercise, Wisconsin National Guard (WING)

Elizabeth Dollar, Emergency Preparedness Program Manager, American Transmission Co.

Greg Engle, PhD, Director, Bureau of Planning and Preparedness, Wisconsin Emergency Management

Mark J. Michie, Brigadier General (ret.), Chief of Staff, Joint Staff, Wisconsin National Guard

Sunset/Vista Ballroom

3:30–4:45 p.m.

Threat Panel

Moderator: Bill Lawrence, VP and CSO, NERC; and Director, E-ISAC

Andy Bochman, Senior Grid Strategist, DOE/Idaho National Lab (INL)

Sam Chanoski, Director, Threat Intelligence and Countermeasures, E-ISAC

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

Ben Miller, Director, Threat Operations Center, Dragos, Inc.

Tim Roxey, VP and Chief Special Operations Officer, NERC

Vikram Thakur, Technical Director, Symantec

Sunset/Vista Ballroom

4:45–5:00 p.m.

Closing Remarks

Sunset/Vista Ballroom

6:00–9:00 p.m.

Evening Networking Reception

Exhibitor Hall (Twilight Ballroom)

Thursday, October 18, 2018 | Solutions Day

7:30–8:15 a.m.

Continental Breakfast

Twilight Ballroom

8:15–9:00 a.m.

International Energy Sector Information Sharing *(panel discussion)*

Moderator: Bill Lawrence, VP and CSO, NERC and Director, E-ISAC

Katsuyuki Abe, Secretary General, JE-ISAC

Jim Linn, Chief Information Officer, American Gas Association and Executive Director, Downstream Natural Gas Information Sharing and Analysis Center (DNG-ISAC)

Johan Rambi, Privacy and Cyber Security Advisor, EE-ISAC

Sunset/Vista Ballroom

9:00–9:45 a.m.

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

Moderator: Ryan Egidi, Technical Project Officer, DOE National Energy Technology Laboratory (NETL)

Dennis Gammel, Research and Development Director, SEL Secure Engineering, Schweitzer Engineering Laboratories, Inc.

Justin John, Technology Director-Controls and Optimization, General Electric Global Research Center

Reynaldo Nuqui, PhD, Senior Principal Scientist, ABB

Sunset/Vista Ballroom

9:45–10:15 a.m.

Break

Twilight Ballroom

10:15–11:15 a.m.

Industry Engagement Program *(panel discussion)*

Moderator: Bluma Sussman, Associate Director, Member Engagement, E-ISAC

Amy Batallones, Information Security Specialist, Security Network Operations Center (SNOC) Lead, Consolidated Edison Company of New York (Con Edison)

Chris Carlson, Major, Superintendent of Law Enforcement, Grand River Dam Authority (GRDA)

Timothy Pospisil, Director, Corporate Security and CSO, Nebraska Public Power District

Matthew C. Stoeckle, Systems Analyst, Corporate Cybersecurity, Nebraska Public Power District

Sunset/Vista Ballroom

11:15 a.m.–1:00 p.m.

Offsite Lunch

Carmine's

Carmine's walking instructions

1:00–2:45 p.m.

Lightning Round of Security Solutions

Sunset/Vista Ballroom

Applying Data Science to Cybersecurity Metrics

Jason Christopher, Chief Technology Officer, Axio Global

Maya Wilson, PhD, Data Scientist, Axio Global

Information Technology (IT)/Operational Technology (OT) Convergence

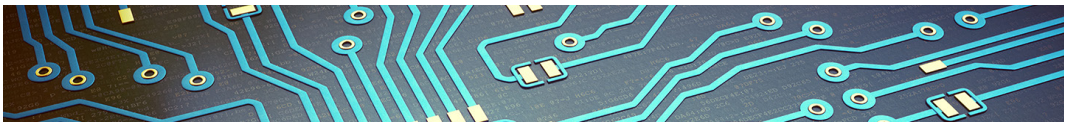
Rafael Oquendo, Information Security Analyst, Con Edison

Linking Cyber Threat Intelligence, Risk Management, and Security Operational Activities

David Zacher, Cyber Risk Services Specialist Lead, Deloitte

Substation Security and Asset Monitoring

Michael Chaffee, Director of Business Development, FLIR Systems, Inc.



The Next Big Threat Starts in the Home

Andrew Marshall, PhD, Portfolio Director, DER Management, Landis+Gyr

Todd Wiedman, Director, IT Security, Landis+Gyr

The Future of Firewall and Network Access Control

Robin Berthier, PhD, President, Network Perception

The Future of IT and OT Converged Orchestration

Andrew Storms, VP of Product, New Context Security

Physical/Perimeter Security Risk Mitigation

Keith Bobrosky, Senior VP, Delta Scientific Corporation

Philip Emerson, VP of Operations, Tusco Inc.

Brent Martina, President, Tusco Inc.

First Break All the Rules: Using Agents to Manage Vulnerabilities

John Livingston, CEO, Verve Industrial Protection

2:45–3:15 p.m. — **Break**

Twilight Ballroom

3:15–4:15 p.m. — **Physical Security Outlook** *(panel discussion)*

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

John Ivemeyer, Substation Engineering Manager, Southern Company Transmission

Tom O'Neill, Senior Manager, International Security, Threat and Risk Assessment, and Corporate Emergency Planning, Hydro-Québec

Kristen Worosz, Senior Analyst

Sunset/Vista Ballroom

4:15–5:00 p.m. — **GridEx V** *(panel discussion)*

Moderator: Jake Schmitter, Senior Manager, Training and Exercises, E-ISAC

Steven Briggs, Senior Program Manager, TVA

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

Douglas Flood, Lead Associate, Booz Allen Hamilton

Sunset/Vista Ballroom

5:00–5:15 p.m. — **GridSecCon 2018 Closing Comments**

Sunset/Vista Ballroom

Friday, October 19, 2018 | Tours and Briefings Day

7:30–8:00 a.m.	**Continental Breakfast** *Twilight Ballroom*
8:00–9:30 a.m.	***Threat Briefing (For Official Use Only)** *Laughlin II and III*
10:00 a.m.–Noon	***Classified Briefing (secret clearance required, Transportation provided)** *FBI Las Vegas* *1787 W Lake Mead Blvd* *Las Vegas, NV 89106*
10:00 a.m.–1:00 p.m.	***Switch Tour** **(55 seats)** *Bus leaves at 10:00 a.m. Tour is 10:30 a.m.-12:30 p.m. Lunch will be provided. Bus returns at 1:00 p.m.*
10:00 a.m.–2:00 p.m.	***Hoover Dam Tour** **(50 seats)** *Bus leaves at 10:00 a.m. Tour is 11:00 a.m.-1:00 p.m. Lunch will be provided. Bus returns at 2:00 p.m.*

* All tours and briefings require advanced registration and confirmation.

Training Track Descriptions

Track 1A and 1B: CyberStrike Workshop

DOE/INL
All-day session, 80 seats available, starts at 8:00 a.m.
Audience: Energy sector owner and operator staff, specifically control room OT personnel, critical infrastructure protection-focused technical staff, energy management system support, operating personnel, and cyber security staff

The DOE's Infrastructure Security and Energy Restoration Division, in collaboration with the E-ISAC and INL, developed the CyberStrike workshop to enhance the ability of energy sector owners and operators in the United States to prepare for a cyber incident impacting industrial control systems (ICS). The training offers attendees a hands-on, simulated demonstration of a cyber attack that draws from elements of the 2015 and 2016 cyber incidents in Ukraine. The instruction platform challenges course participants to defend against a cyber attack on the equipment they routinely encounter within their ICS.

Hands-on labs/modules include the following:

- Open source intelligence
- Denial of service
- Controlling the human machine interface (HMI)
- Bypassing HMI
- Firmware analysis
- Passive man-in-the-middle attack
- Active man-in-the-middle attack
- Defender mitigations

Track 2A: Physical Security Workshop I

E-ISAC Physical Security Partners
Half-day session, 60 seats available, starts at 8:00 a.m.
Audience: Physical security professionals, asset owners, and operators

This track explores issues that affect the physical security of the electricity industry. It allows participants the opportunity to hear a variety of perspectives from physical security experts about topics of importance, such as current issues, best practices, and other issues of audience concern.

Attendees will learn about the following:

- **Drones/Emerging Technology, Foreign Investments**

  Travis Moran, SRC/Gryphon Sensors, will discuss trends in drones and emergent technologies as well as foreign investments and how they impact the security of the electricity industry.

- **Running on a Shoestring Budget**

  Nick Weber, Grant County Public Utility District (Grant County PUD), will provide a case study example of running a security department on a limited budget and discuss lessons learned. In January 2016, Grant County PUD had one staff member in its Security department. Its operating budget of $350,000 was allocated to secure two large hydroelectric plants, 450 miles of transmission line, and a distribution system for 47,000 customers. A new security manager and security coordinator brought fresh perspectives and approaches, notably using enterprise security risk management principles to maximize the value of each dollar spent. Two years later, Grant County PUD has roughly doubled security spending, has tripled its guard coverage, updated camera systems, developed a 24/7 security operations center, and changed its security culture. This session will provide a review of the steps taken and lessons learned in this transformation.

- **Intelligence Sharing vs. Information Sharing**

  John Bryk, DNG-ISAC, will share perspectives on how intelligence sharing differs from information sharing, stressing that understanding can improve your ability to assess threats. The downstream natural gas sector shares much of the same operating environment and threats as the industry.

Track 2B: Physical Security Workshop II–Design Basis Threat (DBT)

PNNL
Half-day session, 60 seats available, starts at 1:00 p.m.
Audience: Physical security professionals, asset owners, and operators

This track demonstrates the use of the *Design Basis Threat Implementation Guide* and how to use the methodology to assess and improve the security of industry assets. The PSAG created the *Electricity Sector Design Basis Threat* to tailor the DBT methodology to industry. DOE, through the Pacific Northwest National Laboratory (PNNL), developed the *Design Basis Threat Implementation Guide* as a companion product designed to assist owners and operators in using the DBT methodology to assess the physical security of their assets. This approach yields actionable results that can be either qualitatively or quantitatively defined, and provides a sound basis for decisions on risk acceptance or upgrade investments.

The DBT guide uses the Vulnerability to Integrated Security Analysis (VISA) process to show vulnerability assessment practitioners how to implement a DBT. The VISA methodology is one of many vulnerability assessment tools that can use a specified DBT to determine the overall system effectiveness of an integrated physical protection system. VISA looks at the functions of detection, delay, and response to baseline a physical protection system to determine cost-effective upgrades. VISA is a cost-effective methodology relying on subject matter expert input to help determine overall system effectiveness.

The goal of this session is to demonstrate how to use these products and help participants gain familiarity with the tools. *Rob Siefken,* PNNL, will provide step-by-step instructions on how to use the guide to assess the security of a generic facility.

Agenda include the following:

- Explanation of DBT and *Design Basis Threat Implementation Guide*
- Sample run of implementation guide
- Discussion of the software tool being developed by DOE

Track 3A: Asset Management for Energy Providers

NCCoE, NIST
Half-day session, 60 seats available, starts at 8:00 a.m.
Audience: Cyber security professionals and ICS owners

Monitoring and managing OT assets is an essential component of protecting the nation's critical infrastructure from cyber attacks. To properly assess cyber security risk within the OT network, energy providers must be able to identify and maintain a complete and accurate view of their OT assets, especially the most critical assets.

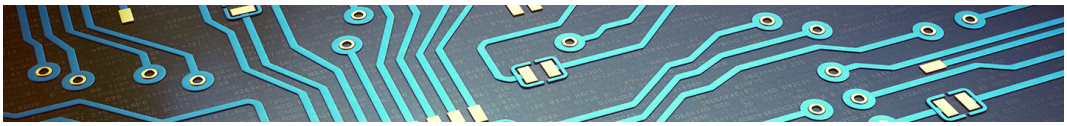
The NCCoE, a part of NIST, is working in collaboration with members of the energy community and cyber security technology providers on an OT asset management example solution to address this complex challenge. This project will result in a NIST cyber security practice guide (Special Publication 1800 series) that shows how commercially available products can create an example solution for electric utilities and for oil and natural gas companies to effectively track and manage their assets. NIST will release this guide in in March 2019.

Join security engineers from the NCCoE NIST, alongside the projects' leading collaborators, for a detailed description of this project and other ICS cyber security projects. The panel will share their expertise and best practices on asset management for the energy sector as well as their current efforts in documenting and implementing methods for managing, monitoring, and baselining assets and information to help identify potential threats to OT assets. Additionally, this conversation will expand to include a panel discussion on Industrial Internet of Things cyber security challenges within the energy sector.

Track 3B: Next-Generation Cybersecurity for Electric Utility OT Networks

Palo Alto Networks, Southern Company, Securicon
Half-day session, 50 seats available, starts at 1:00 p.m.
Audience: Cyber security professionals and ICS owners

This training is presented by utilities and OT cybersecurity practitioners and focuses on the application of next-generation firewalls, advanced endpoint protection, adjacent technologies within electric transmission and distribution, generation infrastructure with the purpose of maximizing visibility, reduction of attack surfaces and the prevention of sophisticated attacks, and malware. The training features a combination of lecture, case studies, and hands-on exercises in a virtual ICS/supervisory control and data aquisition (SCADA) environment.



Track 4A: Build a Security Awareness Program Your Employees Will Love

Curricula, LLC
Half-day session, 40 seats available, starts at 8:00 a.m.
Audience: Cyber security professionals

Many organizations have security awareness programs. But are they looking at the emotional intelligence behind their designs? How do you make your employees love security? Change your focus to get employees to become your best defense and give them the tools to succeed.

Attendees will learn about the following:

- **Section 1: Introduction to Security Awareness Elements**

  Security awareness starts with understanding the basic principles behind psychology and human behavior. Changing the way we communicate information to our employees is the key to success. This session highlights marketing and advertising principals along with understanding metrics that matter to powerful security awareness programs.

- **Section 2: Building Your Plan**
  Successful security awareness requires a plan. We will walk through how to build your ambassador program and security awareness roadmap and provide detailed information on how to successfully launch a phishing simulation program. This session includes demonstrations of detailed phishing simulation tests and how to approach the ongoing exercise of phishing prevention training. We will review the following guides:
  - Security awareness program assessment
  - Security awareness ambassador program
  - Phishing simulation best practices
  - Phishing lessons learned
  - Phishing recovery questions
  - Metrics for executives

- **Section 3: Case Study and Best Practices**
  Time to put all your new knowledge to use. Review case studies that require thinking outside the box and being creative. There are no right answers here, but the group will scrutinize historically predictable approaches. This session will explain best practices from successful security awareness programs. Your new perspective will give you the insight, tools, and motivation to start making a change in your own security awareness and phishing simulation program.

Track 4B: How to be an Exercise Master Planner

TVA
Half-day session, 40 seats available, starts at 1:00 p.m.
Audience: Open to all

Through gamification, a company's cyber security, physical security, and operational response exercises can be an exciting and engaging adventure that people will talk about for years to come. This training takes participants through an overview of the exercise planning process outlined in the Federal Emergency Management Agency Homeland Security Exercise and Evaluation Program process mixed in with elements of tabletop gaming campaign building. The workshop goal is to evolve the way the community holds exercises.

This training event will help planners start working on GridEx V plans. Information learned can be applied to drills, such as phishing, emergency response, and multiple scenario injects.

During this course, the participants will develop an exercise plan that they can communicate to management and other members, allowing for further development and utilization at their companies. They will receive a set of tabletop scenarios, a sample pack of network maps, corresponding city map "game boards," and other material.

Track 5A: Cybersecurity Training for SCADA using Testbed

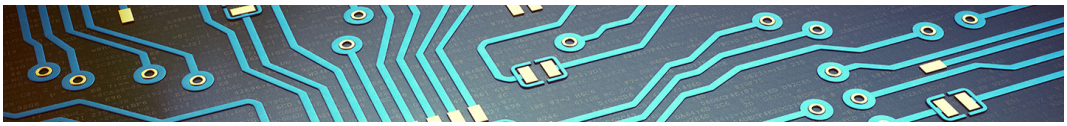
Iowa State University
Half-day session, 24 seats available, starts at 8:00 a.m.
Audience: Cyber security professionals

This session provides a scenario-based, hands-on training experience in cyber attack defense methodology aligning with NERC Critical Infrastructure Protection. The training leverages an industry-grade SCADA platform (Siemens), relays/phasor measurement units (SEL and Siemens), and state-of-the-art security tools and practices (E-ISAC, NIST, DHS).

The training has the following four modules:

- Module 1: Network reconnaissance using Nmap tool
- Module 2: Vulnerability assessment using OpenVAS tool
- Module 3: Vulnerability exploitation, such as "tripping the relay" via sending malicious packets (Wireshark tool)
- Module 4: Defense techniques–network monitoring, firewall, and intrusion detection systems–using Security Onion security information and event management tool

The participants will experiment with real platforms for attack-defense training. This session includes an illustration of real-world scenarios, like the 2015 Ukraine grid attack and potential defenses. Iowa State University conducted similar training sessions at GridSecCon 2015 and 2016 as well as other venues for industry professionals.



Track 5B: Real-Time Threat Response

Tanium
Half-day session, 60 seats available, starts at 1:00 p.m.
Audience: Cyber security professionals

This session provides participants with a high-level overview of the Tanium platform as well as a more technical, hands-on conversation on threat hunting and incident response with the Tanium Threat Response toolset.

Attendees will learn the following:

- How to query information about hosts in a lab environment to quickly triage threats
- The importance of being able to investigate suspicious activity on hosts with accurate, complete information
- How to perform threat hunting processes with Tanium Threat Response using real examples

Track 6A: Social Engineering and Open Source Intelligence (OSINT) Workshop

EC-Council
Half-day session, 95 seats available, starts at 8:00 a.m.
Audience: Cyber security professionals

This training focuses on how hackers use social engineering to get the information they want and how you can defend against social engineering. Attendees will learn about the following:

Fundamentals of OSINT

- OSINT overview
- Where OSINT can be gathered
- Understanding gathering techniques
- Gathering OSINT on people
- Ethical and legal considerations
- Understanding privacy
- LAB: Gathering people OSINT

Fundamental Social Engineering

- Social engineering overview
- Principles of persuasion
- Types of social engineering
- Ethical considerations
- Social engineering as it pertains to “the hack”
- LAB: Interpersonal communications and pretexting

Applied Social Engineering

- Creating payloads
- Cloning and standing up phishing web servers
- Automated phishing solutions
- Spoofing calls for vishing
- Physical security and baiting
- Tailgating
- Applying the concepts to gain access
- LAB: Phishing, vishing, and baiting

Track 6B: Who's in Your Network and How Long Have They Been There?

Burns & McDonnell
Half-day session, 95 seats available, starts at 1:00 p.m.
Audience: Cyber security professionals and ICS owners

In the current state of cyber security affairs, a common theme is the time elapsed between compromise and detection. In many cases, time to detection can be days, weeks, or even months. This course lays out a foundation of distribution, transmission and generation communications, and how a communications network may be implemented to avoid weak points inherent to its design. It identifies the importance of understanding the traffic within a network and how logging, monitoring, and alerting provide visibility into potential attack surfaces. The course also introduces the concepts of attack trees and kill chains and how they can help create insight into an adversary's objectives.

Tour Descriptions

Switch
Switch is the largest data center ecosystem in the world and Las Vegas is home to its Tier 5® Platinum rated multi-tenant/co-location data centers. With capacity of approximately two million square feet of data center space and capacity to deliver up to 315 MW of power, it is the most advanced and most efficient data center campus in the world.

Hoover Dam
Hoover Dam and Lake Mead, spanning the Arizona–Nevada state line, are located in the Black Canyon of the Colorado River about 35 miles southeast of Las Vegas. The dam is a concrete structure that is 726.4 feet high and 1,244 feet long. The dam contains 3.25 million cubic yards of concrete; total concrete in the dam and its secondary buildings is 4.4 million cubic yards. The Hoover Dam was built during the Great Depression and stands as a world-renowned structure. The dam is a National Historic Landmark and the American Society of Civil Engineers has rated it as one of America's Seven Modern Civil Engineering Wonders.

Speaker Profiles

Katsuyuki Abe
Secretary General
JE-ISAC

Katsuyuki Abe supports board members of JE-ISAC as the secretary general, a position he has held since the group's establishment in 2017. Abe leads organizational activities to strengthen cyber security measures of each member company. JE-ISAC provides several face-to-face working group activities, such as sharing cyber security challenges and finding their solutions. Abe is also the general manager of the information systems and telecommunications department of the Federation of Electric Power Companies of Japan and attends various meetings concerning cyber security policies in Japan as the representative of electric power companies. He contributed to the formulation of the National Center of Incident Readiness and Strategy for Cybersecurity's "The Cybersecurity Policy for Critical Infrastructure Protection (4th Edition)" last year.

Abe has a bachelor's degree in Telecommunication Engineering from Tohoku University in Japan. He majored in surface acoustic wave engineering and also has several information security and audit qualifications.

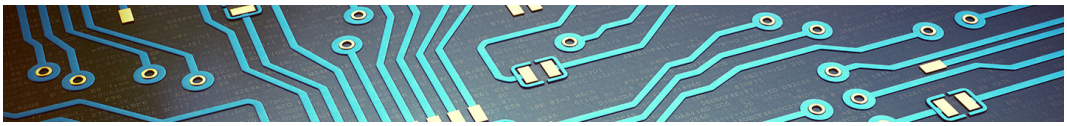
Amy P. Batallones
Information Security Specialist, Security Network Operations Center (SNOC) Lead
Con Edison

Amy P. Batallones is an information security specialist at Con Edison, one of the largest investor-owned energy companies in the United States. Batallones is currently working as the team lead for Con Edison's SNOC, which provides 24/7 analysis, monitoring, and response to potential cyber security threats. Prior to her position as SNOC lead, Batallones worked for four years in information security risk management and was responsible for planning secure architectures for information and OT systems, conducting vulnerability and risk assessments, and drafting cyber security policies.

Batallones has a Bachelor of Science in Computer Science from Fordham University. She specializes in cyber security risk management within the utility industry and has experience in designing and implementing cyber security solutions for both OT and corporate environments. Batallones serves on the executive committee of the IEEE New York section.

Robin Berthier, PhD
President, Network Perception
Research Scientist, Information Trust Institute, University of Illinois–Urbana-Champaign

Robin Berthier, PhD, is the president of Network Perception and a research scientist in the Information Trust Institute at the University of Illinois at Urbana-Champaign, where he has been studying system and network monitoring solutions for critical infrastructures since 2009. He received his doctorate in the field of cyber security from the University of Maryland College Park in 2009. His research projects included the design and development of a honeypot solution for a large campus network and a specification-based intrusion detection sensor for millions of smart meters deployed in advanced metering infrastructures. Berthier is now leading the team at Network Perception to design and develop state-of-the-art monitoring solutions for cyber security and compliance of IT and ICS networks.



Keith Bobrosky
Senior Vice President
Delta Scientific Corporation

Keith Bobrosky has been with Delta Scientific for more than 11 years and has directed Delta's sales team and managed barrier programs for the FBI, CarMax, and the U.S. Department of State's Overseas Building Operations. Currently, Bobrosky takes a more active role in production management, engineering, and business development as senior VP and is focused on efforts promoting the Delta brand and legendary name by furthering clients' requirements for secure perimeter safety and eliminating the concerns for vehicles used as weapons.

Bobrosky has experience designing anti-terrorism vehicle barricade systems for hundreds of government and commercial facilities. In addition, he is the main conduit of communication to most policy decision makers involved with the regulation, testing, and certification of vehicle barrier systems in the United States.

Andy Bochman
Senior Grid Strategist
DOE/INL

Andy Bochman provides strategic guidance on topics at the intersection of critical infrastructure security and resilience to senior leaders in the United States, international government, and industry. His career began in the U.S. Air Force, and he worked for several cyber security start-ups before joining INL. He was the Global Energy and Utilities Security Lead at IBM and a Senior Advisor at the Chertoff Group in Washington, D.C. A member of the global advisory board for the Control Systems Cyber Security Association International, Bochman is on the advisory committee to the SANS security training institute and a cyber security subject matter expert listed with the Department of State Speakers Bureau. In 2018, his publications include "The Missing CSO" (CXO), "Internet Insecurity: the Brutal Truth" (HBR) and "Supply Chain in the Software Era" (the Atlantic Council). LinkedIn: https://www.linkedin.com/in/andybochman/ Twitter: @andybochman

Michael Bowen
Associate Director, Physical Security
E-ISAC

Michael Bowen is an associate director of physical security at the E-ISAC. Bowen directs and develops physical security initiatives and analysis for the entire North American power grid. Prior to joining the E-ISAC, he was the program manager for the Critical Infrastructure Information Sharing Environment and the sector-specific agency representative for both the chemical and dams sectors. 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 nine years and currently serves 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. Briggs served five years as an infantryman in the U.S. Army 2-14 Infantry Battalion, 10th Mountain Division, Fort Drum, New York, rising to the rank of sergeant. While serving, he completed two tours of duty to Iraq as part of Operation Iraqi Freedom 1 and 2.5 and a six-month peace keeping operation to Kosovo.

Briggs is a graduate of the University of Tennessee at Chattanooga with a Computer Science Information Security and Assurance degree with a major in Software Applications. He earned the Global Information Assurance Certificate Response and Industrial Defense, Certified Information Systems Security Professional, Certified Authorization Professional, and Software Engineering Institute CERT-Certified Computer Security Incident Handler certifications.

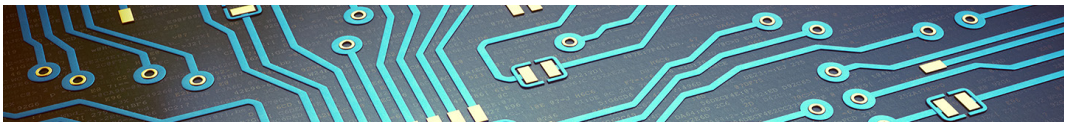
G. David Brown Jr., Lieutenant Colonel
Deputy Director of Domestic Operations for Planning, Training, and Exercise
Wisconsin National Guard (WING)

Lieutenant Colonel G. David Brown Jr., currently serves as the Wisconsin National Guard deputy director of domestic operations for planning, training, and exercise. He is responsible for support to civil authorities to include the planning, coordination, and integration of all aspects of domestic operations in support of natural or man-made disasters. Brown oversees joint domestic operations education, training, exercises, and assessments to deter, prevent, and mitigate threats and aggression within the State of Wisconsin while establishing relationships with valued governmental organizations, public entities, and private industries on behalf of the Wisconsin National Guard. As the vice chair of the WI Utilities P3, Brown has highlighted the importance of integrated ICS training and the conjoint planning of national/state level utilities centric exercises inclusive of GridEx IV, SIMCOM, Dark Sky, and GridEx V.

Chris Carlson, Major
Superintendent of Law Enforcement
GRDA

Major Chris Carlson currently oversees the GRDA Police Department, Physical Security Department, and 24-hour Police Dispatch (approximately 100 sworn full- and part-time officers and 10 non-sworn civilians). Prior to his 17-year police career, Carlson served in the U.S. Air Force for four years.

Carlson received his master's degree in Business Administration in 2017, a bachelor's degree in Law Enforcement Administration in 2015, and associate's degrees in Policing and Option Accounting. Carlson has been the subject matter expert on physical security standards relating to NERC CIP and 693 Standards for GRDA since 2010.



Mike Chaffee
Director of Business Development
FLIR Systems, Inc.

Mike 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. Chaffee has witnessed the growth of FLIR technology in use 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. Chaffee earned a bachelor's degree from the University of Wisconsin.

Sam Chanoski
Director, Threat Intelligence and Countermeasures
E-ISAC

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

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

Chanoski's academic background is in computer science and operations research with graduate degrees in business, engineering, and information security. His professional interests include real-time transmission and distribution operations, organizational behavior, control systems cyber security, and emergency management and resiliency.

Jason D. Christopher
Chief Technology Officer (CTO)
Axio Global, Inc.

Jason D. Christopher's responsibilities as CTO include providing technical leadership on security and resilience issues relevant to Axio, its partners and clients, as well as the development of products for security metrics and benchmarking. Prior to Axio, Christopher led research projects for information assurance at the Electric Power Research Institute. Previously, he was the technical lead for cyber security capability and risk management at DOE and also served as the program lead for both Critical Infrastructure Protection Standards and Smart Grid Security at the Federal Energy Regulatory Commission. Christopher has worked on a variety of infrastructure projects, particularly in the field of industrial control systems design and implementation, where he researched and designed technology systems across multiple industries, including energy, water, transportation, and communications.

Christopher earned a Bachelor of Science in Computer Engineering from the State University of New York at Binghamton and master's degree in Electrical Engineering from Cornell University. He is a SANS instructor and earned a GIAC Critical Infrastructure Protection certification, which complements his expertise is in cyber security for critical infrastructure with a focus on electric and energy organizations.

Tim Conway
Technical Director-ICS and SCADA programs
SANS Institute

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. Conway formerly served as the director of CIP Compliance and OT 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.

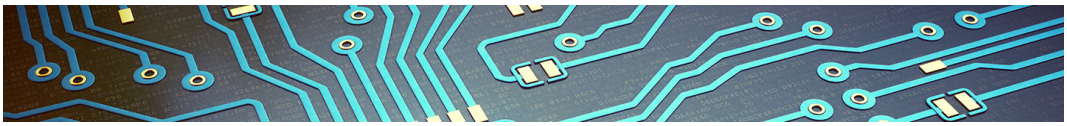
Elizabeth Dollar
Emergency Preparedness Program Manager
American Transmission Co.

Elizabeth Dollar is the emergency preparedness program manager at American Transmission Company, located in Pewaukee, Wisconsin. Dollar manages the program and projects that ensure ATC's compliance with CIP reliability standards set forth by NERC. Since joining ATC in 2008, Dollar has held roles that focus on cost reduction, protection systems, and compliance, including cost control engineer, system protection technical specialist, and senior CIP Compliance project manager.

Dollar has a Bachelor of Science in Business Administration from North Central University, a master's degree in Business Administration from the University of Phoenix, and is a certified Project Management Professional.

Ryan Egidi
Technical Project Officer
DOE, NETL

Ryan Egidi is a technical project officer for DOE's NETL. He is responsible for ensuring the effective stewardship of projects within the Cybersecurity for Energy Delivery Systems (CEDS) program that work toward improving the cyber security posture of the energy sector. Previously, he monitored projects within the Smart Grid Investment Grant program, primarily involving advanced metering infrastructure, communication infrastructure, distribution automation, demand management and cybersecurity. Egidi has a Bachelor of Science in Electrical Engineering from Pennsylvania State University and a Master of Science in Electrical Engineering from Virginia Tech University.



Philip Emerson
Vice President of Operations
Tusco, Inc.

Brent Martina
President
Tusco, Inc.

Philip Emerson, VP of operations at Tusco, and Brent Martina, president at Tusco, have certifications with CVI, JS-anti-terrorism awareness training Level 1, and Department of Defense operational security awareness training. Together they have more than 22 years combined experience with Tusco, Inc., one of the nation's leading perimeter security contractors. Additionally, they both have experience in general contracting. Martina has an undergraduate degree from Birmingham-Southern College with a Business Administration major/Economics minor as well as a master's degree in Building Construction from Auburn University. Established in 1974, Tusco has more than four decades of experience providing local, national, and international customers with perimeter security products. Tusco recently completed multiple physical security substation upgrades with several utility companies in the Southeast and Atlantic coast regions as well as other on-going work with government agencies (such as the FBI), professional and college sports venues, data centers, and other chemical and utility companies.

Greg Engle, PhD
Director, Bureau of Planning and Preparedness
Wisconsin Emergency Management

Greg Engle, PhD, has served as the director of the Bureau of Planning and Preparedness for Wisconsin Emergency Management since 2012. He is responsible for overseeing statewide emergency response planning, training, and exercise programs as well as the State Emergency Operations Center and software systems used statewide to manage incidents. Engle's portfolio also includes building public–private partnerships to improve disaster preparedness among the whole community.

Prior to joining Wisconsin Emergency Management, Engle managed homeland security programs for nine years at the Wisconsin Office of Justice Assistance.

He earned his doctorate from the University of Wisconsin–Madison in 2009 and currently serves as an adjunct professor for emergency management in the Department of Government Affairs and Economic Development at the University of Wisconsin–Green Bay.

The Honorable Karen S. Evans
Assistant Secretary, Office of CESER
DOE

The Honorable Karen S. Evans was sworn in by U.S. Deputy Secretary of Energy Dan Brouillette as the assistant secretary for the Office of CESER on September 4, 2018. Evans was confirmed as assistant secretary for CESER by the U.S. Senate on August 28, 2018.

Before being nominated by President Donald J. Trump to lead DOE's cyber security efforts, Evans served in the public sector as a top IT official at the Office of Management and Budget under President George W. Bush, in the position that is now known as the federal CIO. She has also previously served as DOE's CIO. Most recently, 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. Evans earned a Bachelor of Arts in Chemistry and a master's degree in Business Administration from West Virginia University.

William J. Fehrman
President and CEO
Berkshire Hathaway Energy

William J. Fehrman leads Berkshire Hathaway Energy, a diversified global holding company that owns subsidiaries principally engaged in energy businesses in the United States, Canada, Great Britain, and the Philippines. He previously held executive roles for PacifiCorp Energy, MidAmerican Energy, and BHE Renewables, managed Berkshire Hathaway Energy's cross-business cyber and physical security strategies and served as the lead executive of Berkshire Hathaway Energy's supply chain and procurement initiatives.

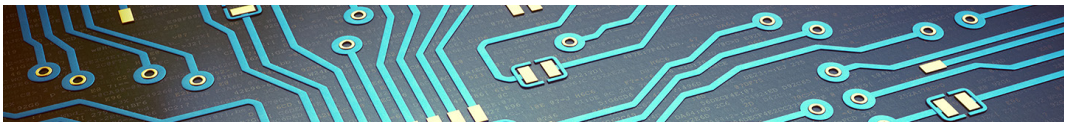
Fehrman graduated in 1984 from the University of Nebraska in Lincoln with a bachelor's degree in Civil Engineering. In 1998, he earned a master's degree in Business Administration from Regis University, Denver, Colo. He is a member of the National Infrastructure Advisory Council and serves as vice chair of the E-ISAC Member Executive Committee.

Douglas Flood
Lead Associate
Booz Allen Hamilton

Douglas Flood, a lead associate with Booz Allen Hamilton's Wargaming and Exercise Team, has more than 10 years of specialized experience in scenario development, exercise design, execution, and facilitation. Flood serves as Booz Allen's project manager in support of NERC's grid security exercise series, GridEx.

Flood also serves as the states' community lead for the Department of Homeland Security's National Cyber Exercise, Cyber Storm, with the responsibility for providing oversight and coordination for all participating states.

Flood earned a Bachelor of Science in International Management from Clemson University. Flood has many years of cyber incident response analytical experience, which he has used to support state, government, and private sector critical infrastructure companies' incident response plans.



Melanie Frye
President and CEO
WECC

Melanie Frye, president and CEO, oversees WECC's mission to effectively and efficiently reduce risks to the reliability and security of the Western Interconnection's Bulk Power System. Frye achieves this work through active interactions with members and key stakeholders by managing relationships with key regulatory and policy-setting bodies and ensuring WECC contributes to a positive relationship with NERC and the ERO.

Prior to this role, Frye served as VP of reliability planning and performance analysis, overseeing WECC's technical and analysis functions, including events analysis, situation awareness, reliability planning and assessments, performance assessments, and standards development. Frye also served as WECC's VP of shared services, overseeing Human Resources, Accounting and Finance, IT, Project Management, and Administrative Services functions and staff. She joined WECC in 2007 as director of human resources.

Before joining WECC, Frye spent several years with PacifiCorp as a senior human resources consultant where she was responsible for providing advice and counsel to the leadership team of eight thermal and three natural gas power generation facilities in Utah and Wyoming. She provided support to more than 2,500 union and non-union employees located across the company's six-state service territory.

Frye earned a Bachelor of Science in Business Administration from Weber State University in Ogden, Utah, and a Utility Executive Course Certificate from the University of Idaho.

Dennis Gammel
R&D Director, SEL Secure Engineering
Schweitzer Engineering Laboratories, Inc. (SEL)

Dennis Gammel is a graduate of the University of Idaho with a Bachelor of Science in Applied Mathematics and has been actively working in the computing and communications industries since 1996. His career experience includes network security design, ICS network architecture, embedded product development, ASIC simulation, and firmware design with RTOS application development. Gammel is presently a research and development director at SEL, responsible for the security technology designed for and implemented in SEL product lines. He has been with SEL since March 2005 and has 20 years of secure firmware and network engineering experience.

Michael Robert Hickok
Assistant Special Agent in Charge
Northern Nevada FBI Las Vegas Field Office

Michael Robert Hickok is responsible for FBI operations in Northern Nevada and for the Cyber and Counterintelligence Programs for the entire Las Vegas Field Office. He joined the FBI in 2002 after having served as an intelligence officer in the U.S. Central Intelligence Agency (CIA) and associate professor of Turkish and Central Asian Studies at the Air War College at Maxwell Air Force Base. He has served in Buffalo and Detroit with two international assignments in Turkey. For leading the FBI's efforts in Turkey against ISIS operations targeting Americans, and during the attempted July 2016 coup, he received the attorney general's Distinguished Service Award in 2017.

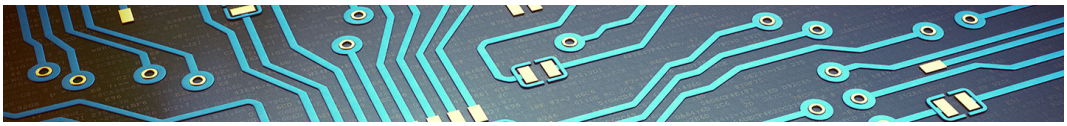
Hickok earned his bachelor's degree in Near Eastern and North African Studies and his doctorate in History from the University of Michigan. Hickok was also an international affairs fellow at the Council on Foreign Relations, 1999–2000, based in Tokyo.

John B. Ivemeyer
Substation Engineering Manager
Southern Company Transmission

John B. Ivemeyer is responsible for all aspects of substation design in the physical and control areas, including design layout, material specification, and construction support across four operating companies. He is also the chair of the Physical Security Committee responsible for security philosophy, vetting security options, CIP-014 compliance, and future electromagnetic pulse solutions. He has held previous roles in NERC compliance, protection and control field services, and transmission maintenance. Ivemeyer earned a bachelor's degree in Electrical Engineering from Georgia Tech. He has more than 30 years of experience in design, operations, commissioning, and trouble response for substations.

Justin John
Technology Director, Controls and Optimization
General Electric Global Research Center

Justin John leads the Controls and Optimization team at GE's Global Research Center. His team is responsible for developing advanced controls, optimization algorithms, and physics-based models to improve the performance and security of GE assets. Prior to joining the Global Research Center in 2014, he was a technical leader with the Controls team at GE Energy and tasked with creating high fidelity power plant models, which were used for design, controls, and operability validation. John has spent a large portion of his career developing advanced controls and models for large combined cycle power plants. John is currently leveraging his controls and physics background together with AI to develop a new way to detect and neutralize cyber attacks on critical infrastructure. He earned a Master of Science in Electrical Engineering from Georgia Institute of Technology.



Bob Kolasky
Director, National Risk Management Center
NPPD, DHS

Bob Kolasky was selected to lead DHS' NPPD National Risk Management Center in 2018. As director, he oversees efforts to facilitate a strategic, cross-sector risk management approach to cyber and physical threats to critical infrastructure. The Center provides a central venue for government and industry to combine their knowledge and capabilities in a uniquely collaborative and forward-looking environment that support both operational and strategic unified risk management efforts.

Kolasky's current position is the culmination of years of risk and resilience experience. He most recently served as the deputy assistant secretary and acting assistant secretary for NPPD's Office of Infrastructure Protection where he led the coordinated national effort to reduce the risk posed by acts of terrorism and other cyber or physical threats to the nation's critical infrastructure, including soft targets and crowded spaces.

Kolasky has served in a number of other senior leadership roles, including acting deputy under secretary for NPPD. In this position, he helped to oversee NPPD's efforts to secure the nation's physical and cyber infrastructure. He has also held a position as the director of strategy and policy for Infrastructure Protection, where he led strategic planning, performance management, and budgeting for the organization and served as director of the DHS Cyber-Physical Critical Infrastructure Integrated Task Force to implement Presidential Policy Directive 21 on critical infrastructure security and resilience as well as Executive Order 13636 on critical infrastructure cybersecurity.

He is also the former assistant director for the Office of Risk Management Analysis at DHS where he was responsible for developing policies and processes to enable risk-informed strategic decisions by DHS. Prior to joining DHS, he was a journalist and an entrepreneur. He helped start two of the first public policy web sites and served as the managing editor for IntellectualCapital.com. Kolasky joined the federal government in 2008 after six years as a management consultant. He graduated from Dartmouth College in 1994 and from the Harvard Kennedy School in 2002.

Bill Lawrence
Vice President and CSO, NERC
Director, E-ISAC

Bill Lawrence, as NERC's VP and CSO 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 joining NERC, 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 service, Lawrence honorably retired from the U.S. Navy with the rank of commander. 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 has a Project Management Professional certification and several cyber security certifications.

Jim Linn
Chief Information Officer, American Gas Association
Executive Director, DNG-ISAC

Jim Linn has spent 30 years in IT and cyber security management. He is currently CIO for the American Gas Association, where he has worked for 20 years. He has administered cyber security reviews with many natural gas utilities and also serves as executive director for the DNG-ISAC. Prior to this, he spent eight years as IT director for the Chemical Manufacturers Association.

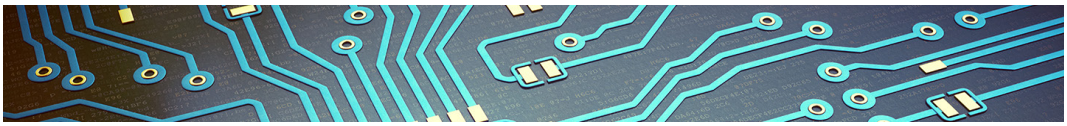
Linn is a Certified Chief Information Security Officer, Certified Information Systems Security Professional, Certified Association Executive, Certified Information Systems Auditor, and has earned other industry certification positions. Linn has a Bachelor of Science in Computer Systems Management from Drexel University and a master's degree in Business Administration from Drexel University.

John Livingston
CEO
Verve Industrial Protection

John Livingston is the CEO of Verve Industrial Protection, a leading industrial cyber security software and services firm. Livingston spent the first 21 years of his career with McKinsey & Company, where he was a senior partner. At McKinsey, Livingston led a range of practices and initiatives: he was the leader of the America's Wireless Telecom practice for four years and the Chicago office for five years, and he was one of the founding members in the firm's advanced analytics practice.

Livingston joined Verve Industrial in 2016 when he partnered with the founder to accelerate the growth of the company's cyber security business. Verve focuses on protecting the critical manufacturing systems that enable production industries (such as power, oil, and natural gas, pharmaceuticals, consumer goods). The company has a 25-year history working in industrial control systems with original equipment manufacterer equipment (such as Siemens, Schneider, Emerson, GE, Rockwell). Verve has applied this experience to providing a vendor-agnostic suite of software and services to bring the best of IT security into the OT environment. Verve's software protects all industrial control equipment from a single, integrated console, providing comprehensive coverage for NIST CSF/NIST 800/IEC 62443/ CIS CSC20 and other standards. The company's services offerings range from assessment and system hardening to ongoing managed security services.

Livingston graduated from Princeton University in 1989 with honors and a degree in Economics. After Princeton, he graduated from Northwestern University Law School and the Northwestern Kellogg Graduate School of Management both in 1993.



Andy Marshall, PhD
Portfolio Director, Distributed Energy Resource Management
Landis+Gyr

Andy Marshall, PhD, is a product leader focused on launching products that enable dramatic improvements to the flexibility of the electricity grid. He currently manages Landis+Gyr's portfolio of distributed energy resource management products and services that control load, generation, and stored energy from the distribution substation to the customer premise. Prior to Landis+Gyr, Marshall served in several product and business development roles with SunEdison and an energy storage start-up, Primus Power.

Marshall started his career with McKinsey & Company leading consulting engagements in technology and operations strategy, and he earned a Bachelor of Science in Chemistry from the University of Notre Dame and a doctorate in Chemistry from Stanford University.

Mark J. Michie, Brigadier General (Ret.)
Chief of Staff, Joint Staff
Wisconsin National Guard

Brigadier General (Ret.) Mark J. Michie is the chief of staff, joint staff and serves as the senior advisor to the state adjutant general for contingency operations. He ensures plans provide for alert, mobilization, deployment, and effective employment of National Guard assets in response to a wide range of either state or federal emergencies. Michie oversees the operations and activities of the joint staff with more than 160 personnel and an annual budget of $65 million. Michie ensures the coordination between the staffs of the respective divisions of the Joint Force Headquarters, Wisconsin, through the chiefs of staff for Army, Air, Wisconsin Emergency Management, and numerous Federal and State agencies.

Ben Miller
Director, Threat Operations Center
Dragos, Inc.

Ben Miller is director, threat operations center 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, he is responsible for performing a threat hunting, incident response, and malware analysis mission for the industrial community.

Previous to his role at Dragos, Inc., Miller was the associate director, E-ISAC and led cyber analysis for the sector. He and his team focused on leading edge cyber activities as they relate to the North American bulk electric system. Miller was recognized as instrumental in building new capabilities surrounding information sharing and analytics in his five years at the E-ISAC. Prior to joining the E-ISAC, Miller built and led a team of nine individuals 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. During this time he also served on a CIP implementation project and various enterprise-wide mitigation programs.

Miller has more than 18 years' experience and currently has CISSP and GIAC Reverse Engineering Malware certifications. Miller has served in various roles including both planner and player roles in GridEx I, II, and III. He served as a member of the NERC Critical Infrastructure Protection Committee Cyber Attack Task Force, an acknowledged contributor to NIST SP 800-150, a panel member of the National Board of Information Security Examiners Advanced Defender panel, and adviser on the CI Advanced Defender Training program.

Miller is an accomplished speaker in various venues including SANS, ICS Joint Working Group (ICS-JWG), ShmooCon, and others. He was recognized by SANS as a 2017 Difference Maker Award Winner for his contributions to the industry.

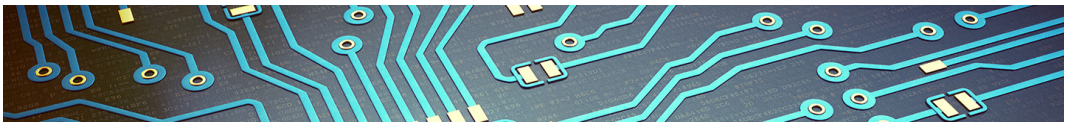
Reynaldo Nuqui, PhD
Senior Principal Scientist
ABB Inc.

Reynaldo Nuqui, PhD, is ABB's subject matter leader in grid resilience. He is the principal investigator of the DOE funded project, "Cyber Attack Resilient High Voltage Direct Current (HVDC) System." In his previous role, he was a system operations engineer at an electric utility. Nuqui earned his doctorate in Electrical Engineering from Virginia Tech in 2001. His background is in grid protection, control, and optimization, including HVDC systems and synchronized phasor measurements.

Tom O'Neill
Senior Manager, International Security, Threat and Risk Assessment, and Corporate Emergency Planning
Hydro-Québec

Tom O'Neill joined Hydro-Québec's Corporate Security team in June 2014. He is currently the senior manager of international security, threat and risk assessment, and corporate emergency planning for Hydro-Québec. O'Neill has played several senior roles in Hydro-Québec's Corporate Security team. Upon his arrival in 2014, he managed physical security covering Hydro-Québec's assets throughout the province and then was senior manager of investigations.

Prior to joining Hydro-Québec, O'Neill spent 27 years with the Royal Canadian Mounted Police (RCMP). In his 27 years with the RCMP, O'Neill had several roles, including deployments to Australia, Iraq, and Indonesia, director general communications for the RCMP, officer in charge of protective operations, planning officer for the North American Leaders Summit, officer in charge of the Montreal Integrated National Security Enforcement Team, and Operations NCO at the Regional Task Force in Montreal.



Rafael Oquendo
Information Security Analyst
Con Edison

Rafael Oquendo, a U.S. Navy veteran, primarily focuses on data leakage and loss prevention, mobile application security, vendor risk assessments, critical infrastructure protection security, and security tool implementation and administration.

Oquendo earned a Master of Science in Computer Science from Hofstra University and an Advanced Project Management Certificate from New York University, which has been used to coordinate with business units and improving processes involving information security and the software development lifecycle.

Oquendo has been a direct contributor with over a decade of experience involving security and technology by meeting SOX, HIPPA, and NERC CIP compliance by providing technical solutions and audit representation.

Timothy S. Pospisil
Director of Corporate Security and CSO
Nebraska Public Power District

Timothy S. Pospisil currently serves as Nebraska Public Power District's director of corporate security and CSO, with responsibility for physical and cyber security for the district. He has been part of Nebraska Public Power District's compliance efforts for the NERC Critical Infrastructure Protection Standards for more than six years and currently serves as Nebraska Public Power District's NERC CIP senior manager. He is active in many groups, including the Large Public Power Council Cyber Security Task Force, the North American Transmission Forum Security Practices Group, and other state and local security groups.

Pospisil joined the team at Nebraska Public Power District in 1999 at Cooper Nuclear Station in Brownville, Neb. where he served as an engineer, and was an employee of Motorola Semiconductor Product Sector, serving as a test and packaging engineer and supervisor in Austin, Texas, and Richmond, Virginia, from 1989 until 1999.

Pospisil earned his Bachelor of Science in Electrical Engineering from the University of Nebraska-Lincoln in 1989. His certifications include: ISACA—Certified Information Security Manager, SANS—GIAC Security Leadership Certification and CompTIA–Security +.

Johan Rambi
Privacy and Cyber Security Advisor
EE-ISAC

Johan Rambi is strategic privacy and cyber security advisor, and he is specialized in the development and implementation of corporate privacy and security policies as well as guidelines and governance structure. Furthermore, Rambi supports organizations with privacy and Data Protection Impact Assessments (DPIAs), privacy and security trainings, definition of security requirements, and implementation of measures in the role of subject matter expert.

Rambi has been active in several European expert groups (e.g., Energy Expert Cyber Security Platform, Network and Information Security platform, DPIA template) for the European Commission on privacy and cyber security. Rambi speaks at conferences in Europe, the United States and Asia about privacy, data protection, smart meter and smart grid cyber security. In December 2015, Rambi launched, as co-founder, the EE-ISAC to promote international collaboration and information sharing through public–private partnership. Also, Rambi supported the Japanese energy sector to set up the JE-ISAC, and Rambi coordinated the signing of the formal partnership between EE-ISAC and JE-ISAC in 2017.

A special highlight for Rambi and recognition of the EE-ISAC was the participation of the G7 Cyber Security Summit in Tokyo in 2016. Finally, Rambi is faculty member of Webster University in Leiden and instructor of the Master of Science in Cyber Security.

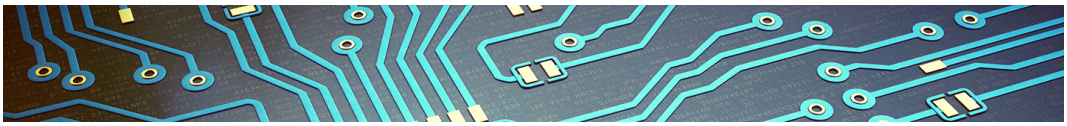
James B. Robb
President and CEO
NERC

James B. Robb assumed the role of president and CEO of NERC in April 2018. He oversees NERC's mission of assuring the reliability and security of the North American bulk power system. As president and CEO, Robb directs key programs affecting more than 1,400 bulk power system 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. Robb also oversees the operations of the regional entities who support the reliability mission across North America.

From 2014 to 2018, Robb served as president and CEO of WECC, where he was responsible for the strategic direction and leadership of all of WECC's activities.

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 VP of enterprise planning and development; at Reliant Energy (now part of NRG Energy) where he served as senior VP of retail marketing for the competitive retail business in Texas and the Northeast; and at McKinsey & Company where he was a partner and the 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.

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



Tim Roxey
Vice President and Chief Special Operations Officer
NERC

Tim Roxey, as NERC's VP and chief special operations officer, is responsible for development and execution of key critical infrastructure protection initiatives, such as NERC's Cybersecurity Risk Information Sharing Program. He also acts as a key coordination point for North American government officials. Roxey also served as interim CSO from November 2017 to August 2018.

Roxey has 30 years of experience in the nuclear utility industry serving in organizations, such as Operations, IT, Licensing, and Security among others. He has more than 45 years of computer-related experience, working in environments from mainframes, minis and micros, to hand-wired special control systems. He has written numerous programs in many different languages.

Roxey is a recognized leader in the fields of security and infrastructure protection formerly serving as deputy chair of the Nuclear Sector Coordinating Council and chair of its Cyber Security Sub-Council. Roxey is the past private sector chair of both the ICSJWG, a position he held for seven years, and the co-chair of the Cross-Sector Cyber Security Working Group.

Roxey spent more than 17 years with Constellation Energy where he was the technical assistant to the vice chair for security-related matters and was involved in a variety of physical and cyber security issues across the nuclear sector of the United States.

As the chief special operations officer for NERC, Roxey is responsible for taking actions to protect the North American grid from both cyber and physical threats.

Jake Schmitter
Senior Manager, Training and Exercises
E-ISAC

Jake Schmitter is the E-ISAC senior manager for training and exercises. He is the exercise lead for GridEx, a training exercise conducted every two years by NERC. GridEx is focused on government and private 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, 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 20 years in the U.S. Navy, both active and reserve. Schmitter has a Bachelor of Science from the U.S. Naval Academy and a Master of Arts from the Naval Postgraduate School. He is a commander in the Navy Reserve.

Matthew C. Stoeckle
Systems Analyst, Corporate Cybersecurity
Nebraska Public Power District

Matthew C. Stoeckle has worked in the IT field for more than 20 years, providing support for fashion retail, global food processing and commodities, and now the electrical utility industry. He has spent the last eight years at Nebraska Public Power District in the Corporate Cyber Security department as a systems analyst.

Stoeckle's role at Nebraska Public Power District focuses on the controlled use of administrative privilege, account monitoring and control, and the specific Center for Internet Security Critical Security Controls related to this work. He takes the Nebraska Public Power District tagline "always there when you need us" seriously and applies this to the work he handles for the people of Nebraska.

Andrew Storms
Vice President, Product
New Context Security

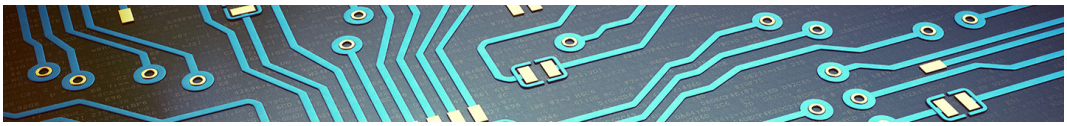
Andrew Storms is the VP, product of New Context Security, an innovator in data security for highly regulated industries. He is a project lead for CES-21, a research initiative around automated cyber security threat detection and response within electrical utility operational networks, and he is a certified information systems security professional. His past roles include senior director of DevOps at CloudPassage and director of information, technology, and security at nCircle.

Storms has more than 20 years in IT security, developing products and solutions for utilities, the enterprise, and government. He is a graduate of the FBI Citizens' Academy, a member of Infragard, and a member of the Open Standards Technical Committee for STIX, TAXII, and OpenC2.

Bluma Sussman
Associate Director, Member Engagement
E-ISAC

Bluma Sussman is an associate director of Member Engagement at the E-ISAC. She works with utility industry executives and analysts, trade associations, and government and international partners to foster a member-focused culture, increase member engagement, and enhance industry's ability to prepare for and respond to cyber and physical threats impacting the North American electric grid. Before joining the E-ISAC in April 2018, Sussman worked for 13 years as a strategy and engagement consultant with Booz Allen Hamilton, leading program implementation and change management efforts across federal government agencies in the national and homeland security space.

Sussman has a Bachelor of Arts in Sociology and Journalism from Brandeis University and a Master of Arts in Media and Public Affairs from George Washington University. She earned a certificate in facilitation from the RIVA Institute.



Vikram Thakur
Technical Director
Symantec

Vikram Thakur is a technical director at Symantec. He leads a team of analysts investigating, researching, and compiling actionable intelligence from the multitude of attacks happening every day. In addition, Thakur liaises research and findings with various global law enforcement agencies and industry partners with the intention of bringing cyber criminals to justice and mitigating online risk for end users. He has held multiple roles within the past 12 years at Symantec, all of which encompassed researching, analyzing, and responding to online threats to better protect end users. He earned a graduate degree in Computer Science from Florida State University.

Todd Wiedman
Director, IT Security
Landis+Gyr

Todd Wiedman is currently responsible for leading the global IT Security program for Landis+Gyr, supporting 72 sites in 31 countries. Wiedman is also responsible for securing and protecting Landis+Gyr's cloud service offering, which includes the hosting of Landis+Gyr's solutions for 300+ customers. Previous to Landis+Gyr, Wiedman had a lead position in the office of the CISO at Dell SecureWorks.

Wiedman has been in IT for 20+ years, with 10+ years working in the cyber security space, and three years in the critical infrastructure space. Wiedman earned CISSP and CRISC security certifications.

Maya Wilson, PhD
Data Scientist
Axio Global, Inc.

Maya Wilson, PhD, since joining Axio, has created numerous cyber program assessment reports, analyzed and provided insights into the cyber maturity of utilities across the United States, and created machine learning models for analyzing and validating data in the Axio platform. Prior to joining Axio, Wilson worked as a researcher while focusing on the politics of funding, advocacy, and policy change with organizations such as the Ford Foundation and has published work on non-governmental organizations and international conflict.

Wilson earned a Bachelor of Arts in Political Science from University of California, Los Angeles, and a Master of Arts and a doctorate in Political Science from Emory University. Her expertise is in quantitative science, including statistics, network analysis, and research design.

Kristen Worosz
Senior Analyst

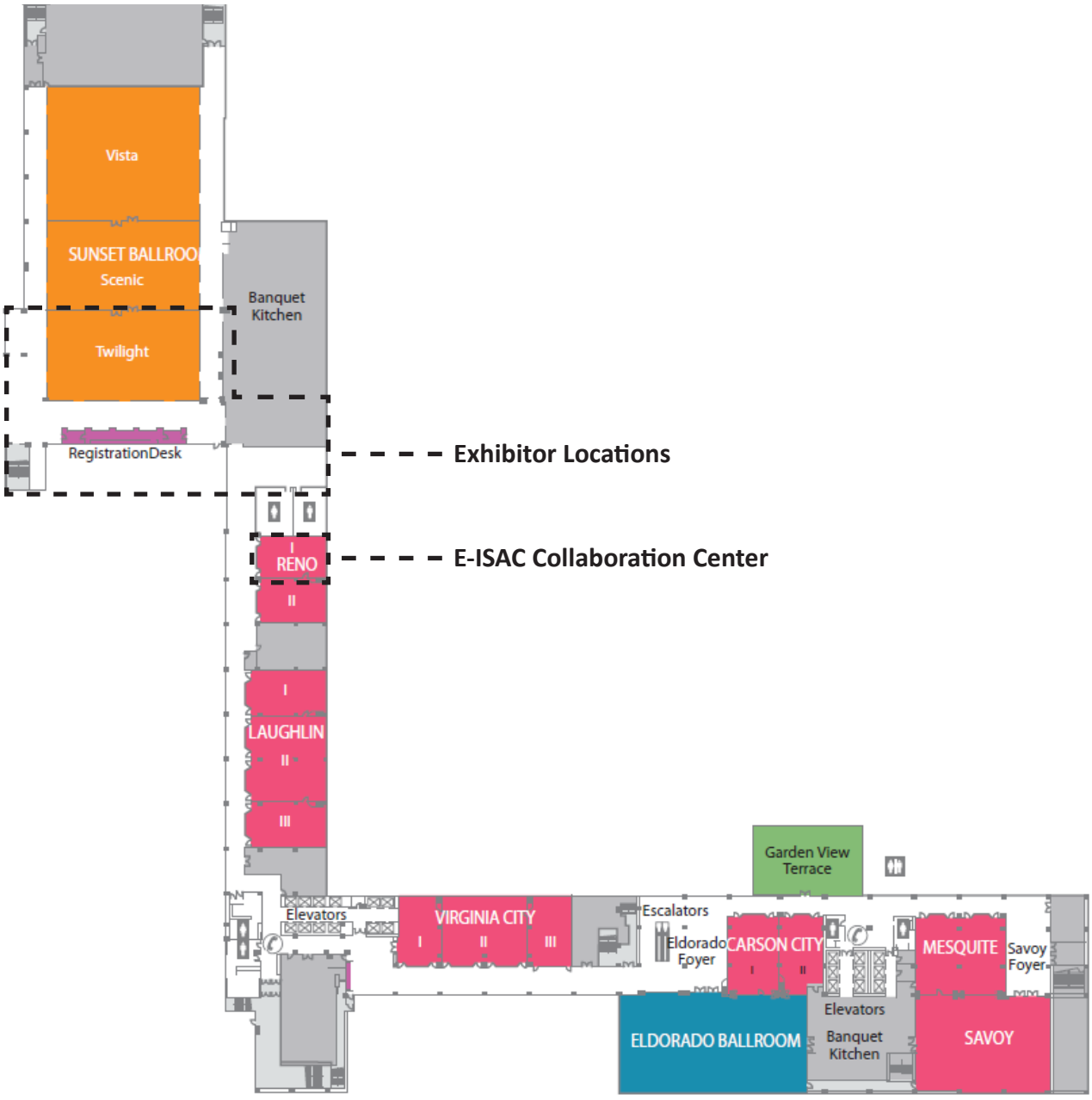
Kristen Worosz has more than ten years of analytical experience in both the federal government and private sector. Worosz is currently a senior analyst, focusing on threats posed by domestic campaign groups, primarily in the Midwest United States, assessing their impact and providing client-focused intelligence on risk management. In her previous position, Worosz was the production manager at the E-ISAC, producing analytical products on the cyber and physical threats facing the electricity industry. Worosz also worked as a counterterrorism intelligence analyst for the FBI and as an analyst in the Investigations Division for the U.S. Department of Justice's Office of the Inspector General.

David Zacher
Cyber Risk Services Specialist Lead
Deloitte

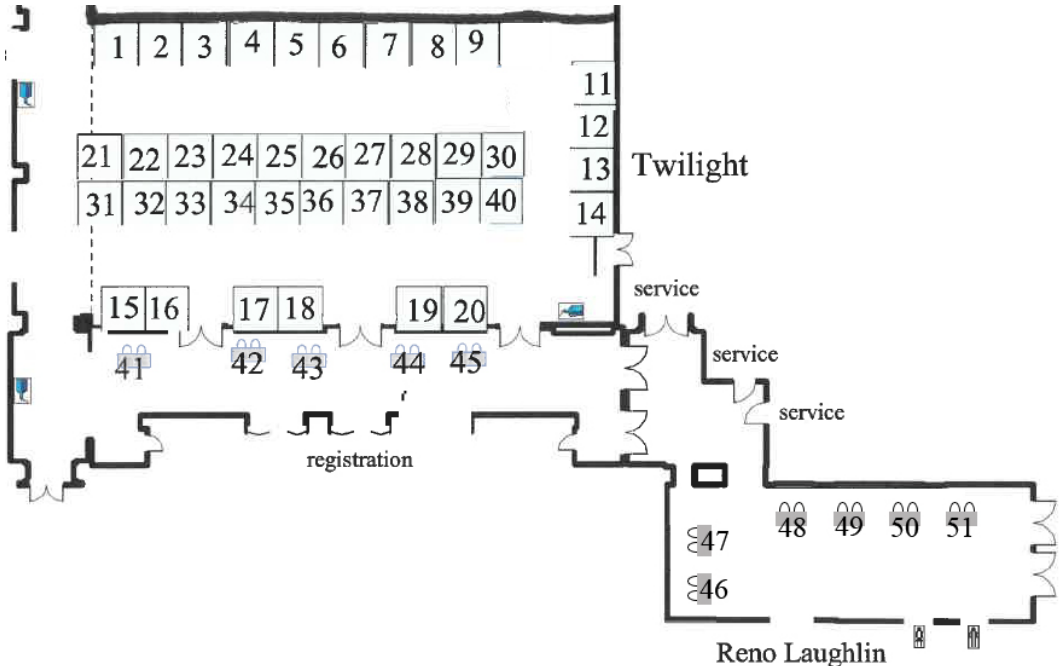
David Zacher is a Deloitte advisory specialist leader with Deloitte's Advisory Cyber Risk Services practice. Zacher has more than 25 years of IT experience with the last 15 years focused on information governance, security, risk management, audit, compliance, access administration, and threat intelligence sharing within the oil and natural gas sector. Zacher served three years as executive director of the Oil and Natural Gas Information Sharing and Analysis Center (ONG-ISAC), providing strategic and operational direction to a member-driven organization that collaborates on cyber threat intelligence relevant to the energy sector, specifically the oil and natural gas industry.

Prior to joining Deloitte, Zacher served for eight years as CISO for a major integrated oil and natural gas company where he was responsible for the development, delivery, and management of cyber security, risk management, and compliance programs. Zacher has served as chairman of the American Petroleum Institute IT Security Subcommittee where he helped to create the ONG-ISAC. Zacher participates in leading industry forums and consortiums to represent business interests and set standards/practices.

Convention Center Map, Third Floor



Twilight Ballroom Exhibition Map, Exhibitors



01	Southwest Microwave	27	VideoTec
02	GridSME	28	AMICO
03	Curricula	29	XTec
04	EC Council	30	Midwest Security Products
05	NIST NCCoE	31	Chain Link Fence Manufacturers
06	Welund	32	Network Perception
07	Palo Alto	33	EnergySec
08	SigmaFlow	34	TDi Technologies
09	Archer Energy Solutions	35	Tanium
11	Security Matters	36	FLIR
12	Owl Cyber Defense	37	Tripwire
13	Perch Security	38	SANS
14	Radiflow	39	Schweitzer Engineering
15	Burns & McDonnell	40	Asymmetric
16	Dragos	41	Subnet
17	IronNet Cybersecurity	42	Iowa State University
18	Claroty	43	Verve Industrial
19	Nozomi Networks	44	Risk Based Security, Inc.
20	ComplyTec	45	ArmorText
21	CAST Perimeter	46	Fortress Information Security
22	Leidos	47	Circadence
23	Veoci	48	Opswat
24	OptaSense	49	Tusco
25	Towerline Software	50	Qnet Security
26	GRESCO	51	AXIO

Platinum Exhibitors

TERRA SOUND TECHNOLOGY

CLAROTY

NOZOMI NETWORKS

Gold Exhibitors

BURNS McDONNELL

ENERGYSEC
SECURING CRITICAL INFRASTRUCTURE

GRIDSME
SUBJECT MATTER EXPERTS

TANIUM

tripwire

Exhibitors

AMICO SECURITY

ARCHER

ARMORTEXT

axio

CAST PERIMETER

Curricula

CIRCADENCE

ComplyTec
ENTERPRISE COMPLIANCE

DRAGOS

CHAIN LINK FENCE MANUFACTURERS INSTITUTE

EC-Council

FORTRESS
Information Security

FOXGUARD SOLUTIONS

IOWA STATE UNIVERSITY

IronNet Cybersecurity

FLIR

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

network perception

GRESCO
TECHNOLOGY SOLUTIONS

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

leidos

OptaSense®
a QinetiQ company

Q-Net Security

OPSWAT.

paloalto NETWORKS

OWL
CYBER DEFENSE

PERCH

radiflow
Secure your Assets

RiskBased SECURITY

SEL
SCHWEITZER ENGINEERING LABORATORIES

SECURITY MATTERS

SIGMAFLOW
NERC Compliance CIP & 693 Solution

SANS ICS

SUBNET SOLUTIONS INC.

tdi technologies

TOWERLINE SOFTWARE, LLC.

TUSCO
PERIMETER SECURITY AND COMMERCIAL FENCING
WWW.TUSCOINC.COM

SOUTHWEST MICROWAVE

veoci

VERVE
INDUSTRIAL PROTECTION

VIDEOTEC

welund
north america

XTEC