GridSecCon 2013 would like to thank:

Platinum Sponsors

CODENOMICON

ALITEK

WATERFALL®
One Way to Connect

Gold Sponsors

Utility Services
You can rely on US!

Owl Computing Technologies

Sponsors

SANS

Corporate Risk®
>>>>>>>SOLUTIONS

SAINT®

QUANTUMSECURE

SECURICON
Information Security Solutions

Raytheon
Trusted Computer Solutions

DSI

AlertEnterprise!

PIKE®

PAS

tripwire

INDUSTRIAL DEFENDER®

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

NERC
GridSecCon 2013

October 15-17, 2013 - Jacksonville, FL

RELIABILITY | ACCOUNTABILITY

Welcome to GridSecCon 2013!

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Welcome to GridSecCon 2013!

Gerry Cauley, President and CEO, NERC

It's my pleasure and distinct privilege to welcome you to the North American Electric Reliability Corporation's third annual grid security conference, GridSecCon 2013. We are excited you are joining us and hope that you will find this year's conference a rewarding experience. I would like to extend a special welcome to our wonderful line-up of speakers for their contributions and our sponsors for helping provide this opportunity.

NERC's mission is to ensure the reliability of the bulk power system, and this year's conference theme, "Threats, Policy, Solutions, and the Bulk Power System" is in direct support of that objective, supplying not only comprehensive discussion on the issues facing the BPS, but also actionable information for mitigating cyber and physical security threats. I encourage you to review the entire agenda and the speaker biographies to fully enjoy the conference's rich subject matter and speakers' diverse expertise.

I hope you're able to take part in one of the four training tracks, either free or greatly reduced in cost. We've been able to line up experts to provide hands-on and topical training in cyber and physical security.

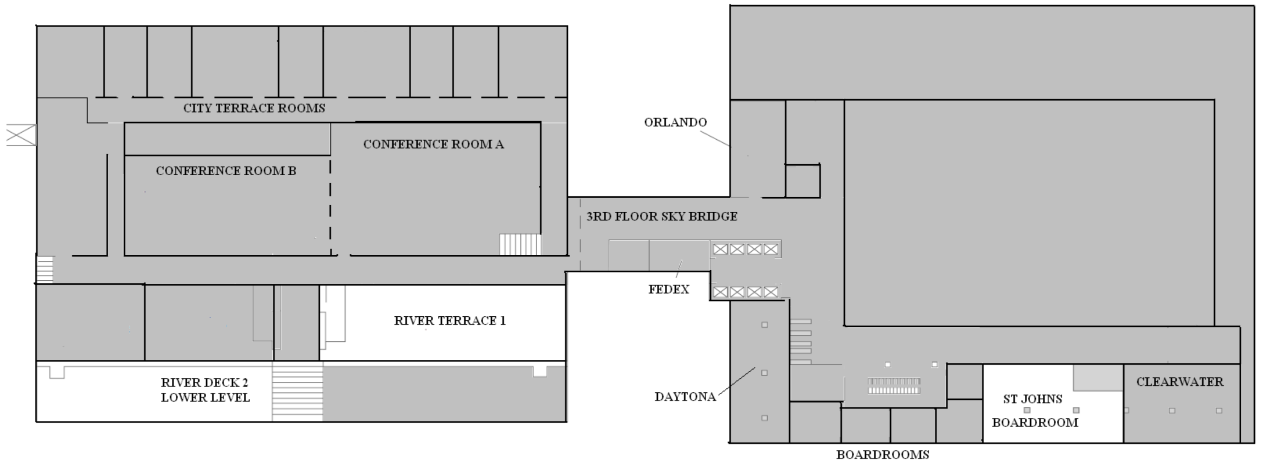
Have a wonderful GridSecCon 2013,

Gerry Cauley

Electronic copies of session slides will be posted after the conference, based on speaker permissions.
Question cards will be distributed – please hand them to a GridSecCon 2013 NERC staff member to carry to the moderator.
Visit the NERC booth at the end of each day to sign the roster to receive recommended CEH hours for the conference.
Please remember, audio and video recording is prohibited during the conference sessions.
Feel free to inform GridSecCon 2013 NERC staff of any issues with the conference spaces or if you see anyone without a conference badge.
Thank you and enjoy the conference!

GridSecCon 2013 Floor Plan

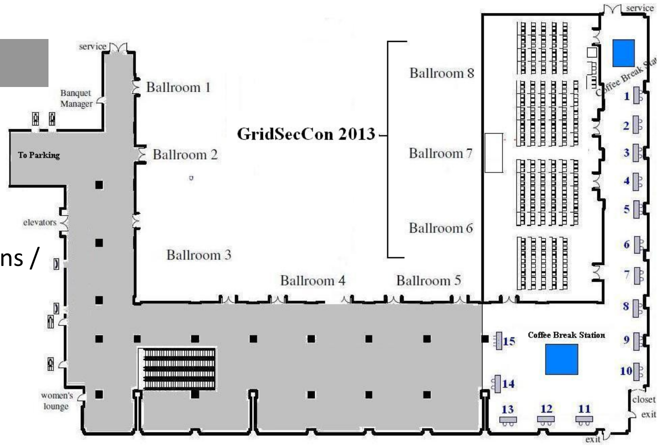
3nd Floor Hyatt Regency Jacksonville



River Terrace 1: Evening Reception (Monday, Wednesday);
Lunch (Tuesday, Wednesday, Thursday)
River Deck 2*—Lower Level: Evening Reception (Tuesday)
** Weather Back-up is Grand Ballroom 1, 2, 3*
St Johns Boardroom: Training Track 1 (Thursday)

2nd Floor Hyatt Regency Jacksonville

Table	Vendor	Table	Vendor
1.	Industrial Defender	**9.**	Quantum Secure
2.	Corporate Risk	**10.**	Tripwire
3.	Raytheon Trusted CS	**11.**	Waterfall
4.	Alert Enterprise	**12.**	Dispersive Solutions / Pike
5.	Codenomicon		
6.	Saint Corp	**13.**	SANS
7.	Securicon	**14.**	PAS
8.	Owl Computing	**15.**	NERC



Grand Ballroom 6, 7, 8: GridSecCon 2013 (Tuesday, Wednesday)
Grand Ballroom 6: Training Track 2 (Thursday)
Grand Ballroom 7: Training Track 3 (Thursday)
Grand Ballroom 8: Training Track 4 (Thursday)
Grand Ballroom Foyer: Breakfast / Breaks / Vendor Booths (Tuesday, Wednesday, Thursday)

Training Tracks

Track 1: CYBATI - Control System Security Hands-On Exercise (free, 42 seats)
Audience - cyber personnel, operations personnel and physical security personnel
Location - 3rd Floor, St Johns Boardroom

CYBATI is offering its flagship, hands-on control system training environment to personnel involved with cyber, physical and operational responsibilities. The day long exercise uses a simulated power grid split among teams constructed of the participants. The teams delegate responsibilities to protect their operations from active threat actors among the other teams. Participants will be briefly educated on the environment, then navigate several stages throughout the exercise prior to summarizing the day's activities. Real industrial controllers, applications, communication protocols and processes will be leveraged within the simulated environment allowing for real world situations. All participants will receive 8 CPEs and an exercise completion certificate. The exercise will include the need for individuals with specific backgrounds to manage specific injects as well as situations arising during the event by active threat actors and normal day to day operations.

Track 2: AliTek - Physical Security (free, 100 seats)
Audience – physical security professionals
Location - 2nd Floor, Grand Ballroom 6

AliTek has developed a comprehensive Physical Security training course focused exclusively on Electric Producers and Transmission Companies. This course combines the CIP standards, industry best practices and other regulatory requirements to assist your company with asset protection, risk management and shareholder value.
CIP-006 Version 3 compliance including six wall enclosures, response plans and all other requirements.

AliTek has extensive industry experience in the electric sector as well as oil and gas, pipeline, distribution and transportation security and risk management. AliTek combines the best security and risk management approaches from government and industry sectors in the course.

Track 3: SANS - Sneak Peek at the SANS ICS 410 Course (discounted to $595, 50 seats)
Audience – technical / cybersecurity professionals
Location - 2nd Floor, Grand Ballroom 7

The SANS ICS 410 course is an ICS Security Essentials focused course that will equip both security professionals and control system engineers with the knowledge and skills they need to safeguard critical infrastructure. While the full course is a 5 day format, SANS will be offering the unique audience of Electric sector cyber security practitioners a sneak peek at the course and specifically the one day of the course that cyber security professionals do not often get to experience - Course Day 2 ICS Attacks. This course day provides the student with an opportunity to learn ICS Attack vectors from Applications, Control Servers, the network, and all the way out to the remote field devices with hands on labs. This sneak peek will also provide students the opportunity to hear an overview of the course topics covered in the full 5 day course.

Track 4: SANS - Compliance Training / Securing the Human (free, 75 seats)
Audience – compliance specialists, trainers, compliance managers
Location – 2nd Floor, Grand Ballroom 8

NERC CIP Versions 1-4 require entities to have training programs for individuals who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The training programs must provide for quarterly security awareness training as well as annual cyber security training on a variety of topics. SANS Institute's Securing The Human now has an awareness training program that addresses these NERC-CIP compliance standards for Utilities.

Securing The Human for Utilities is a computer based training program with 23 security modules that address the most common attack vectors using the 20 Critical Controls as a framework and can be used to satisfy the CIP-004-3-R1 requirement. In addition, there are 7 CIP specific modules that can be used to meet the requirements for CIP-004-3-R2.

This all-day session will walk through CIP V1-4 Training program requirements and demonstrates the SANS training program security awareness offerings as well as walk through the 7 CIP-specific training modules with open discussion around the topics discussed in each. The session will also discuss the direction that the STU program is moving to ensure CIP V5 compliance training requirements in the near future.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

GridSecCon 2013 Agenda

"Threats, Policy, Solutions, and the Bulk Power System"
October 15 – 17, 2013
Hyatt Regency Jacksonville Riverfront, Jacksonville, FL

Monday, October 14, 2013

6:00 – 8:00	**Evening Registration and Reception (3rd Floor, River Terrace 1)**

Tuesday, October 15, 2013

7:30 – 8:30	**Registration and Continental Breakfast (2nd Floor, Ballroom 6, 7, 8 Foyer)**
8:30 – 8:35	Logistics — *Bill Lawrence, Manager of Critical Infrastructure Protection (CIP) Awareness, NERC*
8:35 – 9:00	Welcome Address and Opening Keynote — *Gerry Cauley, President and CEO, NERC*
9:00 – 9:30	Host Utility Keynote — *Paul McElroy, Chief Executive Officer and Managing Director, JEA*
9:30 – 10:15	Security Keynote - *The Honorable Michael Chertoff, Co-Founder and Managing Principal, Chertoff Group*
10:15 – 10:45	**Break (2nd Floor, Ballroom 6, 7, 8 Foyer)**
10:45 – 11:30	Does Anybody Really Know What Time it Is? – *Dr. Michael Cohen, MITRE*
11:30 – 12:15	Sub-station Security: Lessons Learned – *Greg Williams, Security Investigator, Pacific Gas and Electric Company*
12:15 – 1:30	**Lunch (3rd Floor, River Terrace 1)**
1:30 – 2:00	Afternoon Keynote – *Terry Boston, CEO, PJM*
2:00 – 2:45	Threat of Modern Malware— Panel Discussion *Tim Roxey, Chief Cybersecurity Officer and ES-ISAC Director, NERC* *Jonathan Pollet, Founder and Principal Consultant, Red Tiger Security* *Mark Fabro, President and Chief Security Scientist, Lofty Perch* *Billy Rios, Technical Director and Director of Consulting, Cylance*
2:45 – 3:15	**Break (2nd Floor, Ballroom 6, 7, 8 Foyer)**
3:15 – 4:15	How the Grid Will Be Hacked – *Josh Axelrod and Matt Davis, Ernst & Young*
4:15 – 4:45	Electricity Sector Information Sharing and Analysis Center Update — *Tim Roxey, Chief Cybersecurity Officer and ES-ISAC Director, NERC*
4:45 – 5:00	Closing Remarks – *Matt Blizard, Director of Critical Infrastructure Department, NERC*
6:00 – 8:00	**Evening Reception (3rd Floor, River Deck 2—Lower Deck)**

Wednesday, October 16, 2013

7:30 – 8:30	**Continental Breakfast (2nd Floor, Ballroom 6, 7, 8 Foyer)**
8:30 – 9:15	Federal Energy Regulatory Commission's (FERC) Office of Energy Infrastructure Security (OEIS) – *Barry Kuehnle, CIP Senior Advisor, FERC, OEIS*
9:15 – 9:45	Information Sharing Task Force Recommendations – *Stephen Diebold, Senior Director, Ventyx*
9:45 – 10:45	CIP Compliance — Panel Discussion *Tobias Whitney, Manager of CIP Compliance, NERC* *Gregory Goodrich, Supervisor, Enterprise Security at New York Independent System Operator* *Kevin Perry, Director, Critical Infrastructure Protection at Southwest Power Pool Regional Entity* *Roger Fradenburgh, Principal Security Architect, Network & Security Technologies*
10:45 – 11:15	**Break (2nd Floor, Ballroom 6, 7, 8 Foyer)**
11:15 – 12:15	EMP Threat: A DOE Perspective - *Deputy Assistant Secretary Bill Bryan, U.S. Department of Energy*
12:15 – 1:15	**Lunch (3rd Floor, River Terrace 1)**
1:15 – 1:45	The Future of Cybersecurity - *Dr. Andy Ozment, Senior Director for Cybersecurity, National Security Staff*
1:45 – 3:00	Outside the Box - Risk Management Solutions from Off the Shelf - Panel Discussion *Bill Lawrence, Manager of CIP Awareness, NERC* *Bob Twitchell, Dispersive Solutions* *James Anderson, Digital Globe* *David Graham, Owl Computing Technologies* *Andrew Ginter, Waterfall Security*
3:00 – 3:30	**Break (2nd Floor, Ballroom 6, 7, 8 Foyer)**
3:30 – 4:30	A CISSP's Perspective on CIP and Security *- Richard Kinas, Manager of Compliance, Orlando Utilities Commission*
4:30 – 5:00	GridEx II Success Strategy *– Bill Lawrence, NERC*
5:00 – 5:15	Closing Comments — *Brian Harrell, Associate Director of CIP Programs, NERC*
6:00 – 8:00	**Evening Reception (3rd Floor, River Terrace 1)**

Thursday, October 17, 2013

8:00 – 5:00	Each training track will be an all-day session. More information and track descriptions can be found on page 14.
7:00 – 9:00*	**Continental Breakfast**
10:00 – 11:00*	**Break**
12:00 – 1:00*	**Lunch (3rd Floor, River Terrace 1)**
2:00 – 3:00*	**Break**

***Times may vary depending on Training Track Schedule**

Bob Twitchell

Founder and CEO, Dispersive Solutions

Bob has an extensive background in the wireless industry. He holds 48 granted patents with over 40 additional non-provisional patents pending in wireless, GPS, networking and location technology. He is a SME (Subject Matter Expert) for DoD on Mobile Phones and Cyber Warfare.

From October 2007 until the present, Bob is the Founder and CEO of Dispersive Networks, Inc., a Georgia company that is pursuing secure networking and dispersive computing platform. From November 2001, Bob was founder, CTO and consultant of TeraHop Networks, a Delaware company that pursued container tracking and first responder technology. Prior to that, Bob was Chairman and CTO of Intransit Networks, Inc., a Washington startup that pursued inventory tracking and control technology.

Prior to Intransit Networks, Bob was at Nokia, where he served as Value Added Services Manager, CDMA Markets, and was responsible for strategy and implementation of location based services. As Product Program Manager of Value Added Services with Nokia, Bob negotiated contracts with suppliers and subcontractors, put together the team to develop the GPS accessory (3 partnerships and 4 subcontractors), developed a WAP software platform and setup the program for the Nokia 3285. He was responsible for Marketing, After sales, Quality, Manufacturing and R&D in all of his assignments as Product Program Manager. He led the development of the Nokia 9000 "Communicator" for the US market whose record setting 11-month development to market has not been repeated. Bob has a Masters Degree in Electrical Engineering with a Master's Thesis involving DSP, Neural Networks and Voice Recognition.

Greg Williams

Security Investigator, Pacific Gas and Electric Company

Greg Williams has been with Pacific Gas and Electric Corporation for the past two years. He has served as a Corporate Security Investigator and is currently serving as the Assistant Director of Security at Diablo Canyon Power Plant. Prior to PG&E, Greg retired as a Lieutenant with the California Highway Patrol where he concluded his 28 years of law enforcement. During his law enforcement career he served in field assignments as an officer, sergeant, and lieutenant in addition to investigative, supervisory and management assignments on state and federal task forces. He has served as an associate instructor at the CHP Academy in Sacramento and instructed on a variety of topics related criminal investigations both nationally and internationally.

Tobias Whitney

Manager of CIP Compliance, NERC

Tobias Whitney joined NERC in May 2012 as the CIP Compliance Manager and works in the Washington, DC office. He has over 15 years of energy security and audit experience and his role at NERC is to lead the CIP Compliance Audit Oversight function, facilitate and provide administrative support to the CIP Compliance Working Group while providing CIP subject matter expertise as a compliance liaison to the Cybersecurity 706 Standard Drafting Team. Tobias has a long working relationship with the Regions and Registered Entities and has significant auditing and compliance experience. Tobias is a professional trained IT systems auditor from PricewaterhouseCoopers LLC where he functioned as a Senior IT Systems Auditor and performed audit assurance and internal auditing functions for various Fortune 100 businesses. Tobias subsequently worked as an engineer at Burns & McDonnell Engineering in Missouri where he led the Critical Infrastructure Advisory team and GE Energy's Smart Grid Center of Excellence. His responsibilities include integrating cyber security requirements into substations, control centers, power plants and smart grid technologies. He has successfully delivered over 25 NERC CIP Compliance projects and is a past member of the Smart Grid Interoperability Panel and NERC's Control System Security Working Group. He has been an active participant at NERC CIPC and subcommittee meetings since 2004 and was a core member of the Cyber Attack Task Force in 2011. He received top secret clearance in 2006 and a certified information systems security professional accreditation in 2002. Tobias has written papers and presented at T&D World University, DistribuTech, Public Utilities FortNightly, EEI and IEEE. Tobias' educational background includes a BS in Business and Public Administration University of Missouri in 1998 and an executive MBA at Washington University, Saint Louis Olin School of Business in 2010.

Jonathan Pollet

Founder and Principal Consultant, Red Tiger Security

Jonathan Pollet, Founder and Principal Consultant for Red Tiger Security, USA has over 15 years of experience in both Industrial Process Control Systems and Network Security. After graduating from the University of New Orleans with honors and receiving a B.S. degree in Electrical Engineering, he was hired by Chevron and designed and implemented PLC and SCADA systems for onshore and offshore facilities. In 2001 he began to publish several white papers that exposed the need for security for Industrial Control Systems (ICS), and is still active in the research of vulnerabilities within real-time ICS systems. Throughout his career, he has been involved with SANS, IEEE, ISA, ISSA, UTC, CSIA, NERC, and several other professional societies. Pollet has developed and presented workshops on SCADA security to the FBI, Department of Homeland Security, Department of Defense, London CPNI, Canadian PSEPC, and workshops around the world. He has also been featured on Fox News Live, Vanity Fair, Popular Mechanics, CIO Magazine, and several security publications.

Billy Rios

Technical Director and Director of Consulting, Cylance

Billy Rios is the Technical Director and Director of Consulting at Cylance. He provides technical direction and advice on Cylance business operations and strategic decision making. Prior to Cylance, Billy worked as a Lead for Web and Products Security Response at Google and as Founder and CEO of SpearPoint Security Services prior to its acquisition by Cylance. Billy served in the US Marine Corps as an officer from 2000-2004. He holds an MBA in Business Administration from Texas A&M University, an MS in Applied Intelligence from Mercyhurst College, an MS in Information Systems from Hawaii Pacific University, and a BA in Business and Information Systems from the University of Washington.

Orlando Stevenson

Cybersecurity Specialist, Electricity Sector Information Sharing and Analysis Center (ES-ISAC)

Orlando Stevenson is a Cybersecurity Specialist in the ES-ISAC at NERC reporting to Tim Roxey, Chief Cyber Security Officer and Director. Previously, he worked for a large, vertically integrated, state-wide utility for over twenty years focusing on technology infrastructure and cyber security in corporate and operational settings with positions including IT Security Supervisor and IT Consultant. Orlando has a Bachelor Degree in Computer Science/Electrical Engineering (minor) along with two Masters Degrees. His cyber security focus over the last ten years includes attaining a number of professional certifications along the way.

Tim Roxey

Chief Cyber Security Officer, NERC

Tim Roxey is responsible for development and execution of key critical infrastructure protection initiatives, such as NERC's cybersecurity risk preparedness assessment and other continuous risk assessment efforts. Tim also acts as a key coordination point for North American government officials and is the director of the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). Mr. Roxey has over 30 years of experience in the nuclear utility industry serving in organizations such as Operations, Information Technology, Licensing, and Security, among others. Tim has over 35 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. Tim is a widely recognized leader in the fields of security and infrastructure protection, formerly serving as Deputy Chair of the Nuclear Sector Coordinating Council and Chairman of its Cyber Security Sub-Council. Tim is presently the Private Sector Chairman of the Industrial Controls System Joint Working Group (ICSJWG). He is also one of two co-chairs of the Cross Sector Cyber Security Working Group (CSCSWG). Tim spent over 17 years with Constellation Energy. At Constellation Tim was the Technical Assistant to the Vice Chairman for security related matters and was involved in a variety of both physical and cyber security issues across the entire nuclear sector of the United States. In the realm of physical security Tim was involved in reviewing security system architectures for the next generation of nuclear power in America as a member of the various oversight committees. Tim also served, by invitation, on two Presidential Commissions helping to prepare guidance for the next administration.

Biographies

James Anderson

Project Manager and Principal Intelligence Analyst, Digital Globe Analytics

Prior to joining DigitalGlobe in 2009, James spent 20 years in the US Air Force as an all-source intelligence analyst. During this time with DigitalGlobe he has been a principal intelligence analyst and Program Manager. James is part of a team that applies advanced geospatial analytic techniques to address a wide array of problem-sets within both Government and Commercial sectors.

Josh Axelrod

Ernst & Young

Joshua Axelrod is a Senior Manager in the Advisory Services practice of Ernst & Young LLP. He serves as the National Practice Information Security Lead for the Power and Utilities Sector through the Ernst & Young Center of Excellence. Focusing on the needs of business, security, and operations, he aids the Power and Utilities sector to structure its policies, processes, procedures, operational/informational technology infrastructure, and operational/informational and physical security programs to enhance business efficiency, regulatory compliance, situational awareness, and overall security in the dynamic environment facing the sector.

Joshua is a retired United States Navy Submarine Officer with more than thirteen years of operational experience in nuclear power generation, electrical distribution, mechanical systems, and the industrial control systems associated with operation, supervision, and security. Joshua possesses extensive operational auditing experience with respect to generation and distribution operations, infrastructure security, and training. Mr. Axelrod's experience includes regulatory compliance with Department of Defense, Environmental Protection Agency, Occupational Safety and Health Administration, Code of Federal Regulations directives and standards, North American Electric Reliability Corporation standards and requirements, Federal Energy Regulatory Commission requirements, and the National Institute for Standards and Technology guidance.

Terry Boston

President and CEO, PJM Interconnection

Prior to joining PJM, Mr. Boston was the executive vice president of the Tennessee Valley Authority's (TVA) Power System Operations. Mr. Boston joined TVA as a power supply engineer in 1972 and held various leadership positions over the next 35 years. Mr. Boston is chair of the North American Transmission Forum, focused on operational excellence and best practices for the grid. Mr. Boston serves as a U.S. vice president of the International Council of Large Electric Systems, and vice president of the Consortium for Electric Reliability Technology Solutions. He is on the DOE advisory council for the Advanced Research Projects Agency--Energy. He serves on the study group of the National Infrastructure Advisory Council that provides the President and DHS with advice on the security and resilience of critical infrastructure. He has served for six years on the NERC Engineering Committee and Transmission Task Force and currently serves on the NERC Members Committee. Mr. Boston was one of eight U.S./Canadian industry experts selected to direct the NERC investigation of the August 2003 Northeast/Mid-west blackout.

Matt Blizard

Director of Critical Infrastructure Protection, NERC

Matt Blizard joined NERC in May 2011 as the Policy and Coordination Manager for the Chief Security Officer of the Critical Infrastructure Protection (CIP) organization. Mr. Blizard is responsible for overseeing CIP and cyber security program policy efforts and coordinating development and execution of critical infrastructure protection initiatives.

Mr. Blizard comes to NERC after thirty-four years with the Coast Guard, thirty years commissioned service. His experience and education are extremely diverse – leading, managing and achieving multiple commands throughout his Coast Guard career. Opportunities and assignments span assignments within operations, engineering and sustainment, mission support, and policy development. He focused a career on drug supply reduction efforts, building and operating communication and navigation systems, and engineering/logistic support for operations – all from the tactical to the strategic. His most recent achievement included assignment as the Deputy Chief of Staff and Executive Director to the Deputy Commandant for Mission Support of the Coast Guard – extremely focused on the day-to-day operations of the Coast Guard and more specifically on mission support transformation of the Services engineering, human resources, C4IT, and acquisition efforts. Transformational efforts concluded with testing of the Service's new mission support structure with earthquake relief efforts in Haiti and in Deepwater Horizon oil clean-up actions. He designed and built the Coast Guard's Maritime Information Center; consolidated the Atlantic Area's Communication System into a "one-stop shopping" center of communication excellence; prepared the Atlantic Communication System for Y2K concerns; and built the Coast Guard's Command, Control and Communication System for the Exxon Valdez oil clean-up. Matt concluded his Coast Guard career as an Assistant Professor of the National and Homeland Security curriculum at the National War College, National Defense University.

Matt has his BS in Electrical Engineering (BSEE) from the United States Coast Guard Academy; MSEE from Purdue University; MSCS from Rensselaer Polytechnic University (HGC) and his MS in National Security Strategy and Resourcing from the Industrial College of the Armed Forces, National Defense University. Matt is a professional engineer with the State of Washington and has taught Electrical Engineering at the United States Coast Guard Academy.

Bill Bryan

Deputy Assistant Secretary - U.S. Department of Energy

Mr. Bryan is the Deputy Assistant Secretary for Infrastructure Security and Energy Restoration (ISER) in the U.S. Department of Energy's (DOE) Office of Electricity Delivery and Energy Reliability. The ISER works with the National Security Staff, other U.S. government agencies, and international partners to enhance the security and resiliency of critical energy infrastructure and facilitate the reconstruction and recovery of damaged or disrupted energy systems.

As a career Senior Executive, Mr. Bryan oversees the collection, analysis, and dissemination of vital information to all involved in energy response and restoration efforts. Mr. Bryan leads DOE's efforts in the coordination and collaboration of energy sector-related reliability and resiliency activities between the energy industry and the federal government. He also leads the office in support of the electricity, oil, and natural gas industries in the development and implementation of infrastructure protection strategies and methodologies both at home and abroad.

Before assuming his current position, Mr. Bryan served as the Director for Critical Infrastructure Protection (CIP) in the Office of the Under Secretary of Defense for Policy at the U.S. Department of Defense (DOD). He led all CIP and Defense Industrial Base (DIB) related activities within this office, and advised key DOD leadership on the relevance of current CIP and DIB capabilities, methodologies, and technologies in support of military and civil homeland defense efforts deemed essential to national security.

Mr. Bryan holds a Master of Science in Strategic Intelligence from the Joint Military Intelligence College in Washington D.C. He also holds a Bachelor of Science in Logistics Systems Management (Summa Cum Laude) from Colorado Technical University in Colorado Springs, CO.

Gerry Cauley

President and CEO, NERC

Gerry W. Cauley is President and Chief Executive Officer of the North American Electric Reliability Corporation (NERC), effective January 1, 2010. Mr. Cauley had served since 2007 as President and Chief Executive Officer of the SERC Reliability Corporation, a nonprofit corporation responsible for promoting and assessing the reliability and critical infrastructure protection of the bulk power system in 16 southeastern and central states. Previously, Mr. Cauley worked at NERC for ten years in positions of increasing responsibility, ultimately as Vice President and Director of Standards. He was instrumental in preparing NERC's application to become the Electric Reliability Organization and spearheaded NERC's development of an initial set of standards to ensure the reliability of the bulk power system in North America. Mr. Cauley was also a lead investigator of the August 2003 Northeast blackout and coordinated all aspects of the NERC Y2K Program, supervising the reporting and readiness of 3,100 electric organizations in the United States and Canada. Prior to joining NERC in 1996, Mr. Cauley served for six years as the program manager of grid operations and planning at the Electric Power Research Institute. He was also a training consultant for ten years in the

Mr. McElroy currently serves on the boards of The Energy Authority, Inc. ("TEA"), Colectric Partners Inc., Florida Reliability Coordinating Council, Northeast Florida Safety Council, Inc., and the Jacksonville Chamber of Commerce. Mr. McElroy is a member of the American Public Power Association Board's Executive Committee and serves as Treasurer, as well as a member of the Large Public Power Council CEO Roundtable.

Mr. McElroy holds a Bachelor of Science in accounting from St. Joseph's College in Rensselaer, Indiana and a certificate from the Advanced Management Program of the Wharton School of the University of Pennsylvania and pursued graduate level studies at the University of Bridgeport and the University of New Haven in Connecticut.

Before joining JEA, Mr. McElroy served as a Vice President and General Manager for Bombardier Capital Corporation in Jacksonville, Florida and Colchester, Vermont. Prior to that, he served in a variety of management positions with Pitney Bowes Credit Corporation, including Controller, Director – Marketing and Vice President, Internal Finance Division in Norwalk, Connecticut.

Dr. Andy Ozment

Senior Director for Cybersecurity, National Security Staff

Dr. Andy Ozment has worked on cybersecurity as a programmer, operator, researcher, and policymaker. He has coded the authentication security for a mainframe application, built a custom host-based intrusion detection system that caught an intrusion the first night he ran it, developed national cybersecurity policy, and had his personal website hacked (which was a bit embarrassing). Currently, he is the Senior Director for Cybersecurity at the White House and one of two deputies to the Cybersecurity Coordinator.

At the White House, Andy leads a team of individuals who develop national policy and coordinate federal cybersecurity efforts in the areas of critical infrastructure protection, legislative proposals, executive branch security, privacy and civil liberties, information sharing, and incident response. In a prior stint at the White House, Andy led the effort to develop the National Strategy for Trusted Identities in Cyberspace (NSTIC) and established the Administration's priorities for federal agency cybersecurity.

Andy has previously worked at the Office of the Secretary of Defense, National Security Agency, MIT Lincoln Laboratory, and Nortel Networks. He has a PhD in Computer Science from the University of Cambridge, an MS in International Relations from the London School of Economics, and a BS in Computer Science from Georgia Tech.

Kevin Perry

Director, Critical Infrastructure Protection, Southwest Power Pool Regional Entity

Kevin joined Southwest Power Pool, Inc. (SPP) in June 1997 and currently serves as the Director, Critical Infrastructure Protection for the SPP Regional Entity. Kevin is responsible for leading the CIP Standards compliance monitoring and enforcement program activities for the SPP region. Prior to his current role, Kevin was the Director of IT Strategic Projects following several top leadership positions in the SPP Information Technology department. Kevin was instrumental in forming the SPP Critical Infrastructure Protection Working Group and served as its secretary until joining the Regional Entity.

Kevin is the past chair of the NERC Critical Infrastructure Protection Committee, a bi-national security advisory committee for the electricity sector, and was the Vice Chair of the NERC CIP Standards revision (CSO706) drafting team until October 2009.

Kevin came to SPP from Entergy, where he was a Senior Lead System Operations Analyst, responsible for the administration of the Energy Management Systems at the Pine Bluff Transmission System Operations Center. Prior to Entergy, Kevin worked at Empros Systems International, Control Data Corporation, NASA-Langley Research Center, and the US Army Computer Systems Command.

Kevin received a Bachelor of Science degree in Management Information Science from Christopher Newport University and a Master of Arts in Computer Resources and Information Management from Webster University. Kevin is a Certified Information Systems Auditor (CISA). He is also Certified in Risk and Information Systems Control (CRISC).

Brian Harrell

Associate Director of CIP Programs, North American Electric Reliability Corporation

Brian Harrell is the Associate Director of Critical Infrastructure Protection (CIP) Programs Division for the North American Electric Reliability Corporation (NERC), joining NERC in August 2010. In this capacity he is responsible for managing ERO wide critical infrastructure protection standards initiatives and assisting in the development of the overall CIP program strategy.

Mr. Harrell has 15 years of experience in the security industry serving in organizations such as law enforcement, military, and corporate security, among others. Brian is formerly the Manager of Critical Infrastructure Protection for SERC Reliability Corporation where he oversaw all security and CIP reliability related matters for the Region. Prior to joining SERC, Brian was the Sector Security Specialist for the Infrastructure Security Compliance Division at the U.S. Department of Homeland Security (DHS). Brian specialized in securing high risk critical infrastructures and Continuity of Operations (COOP) for DHS. Brian also served in the US Marine Corps as an Anti-Terrorism and Force Protection Instructor and has an MA from Central Michigan University and a BA from Hawaii Pacific University. He is also board certified in security management.

Richard Kinas

Manager of Compliance, Orlando Utilities Commission

Rich Kinas is the Manager of Standards Compliance at Orlando Utilities Commission. He was a member of the FERC Order 706 Cyber Security Standard Drafting team for CIP versions 2, 3, 4, and 5. He is a member of the NERC Operating Committee, chair of the FRCC Compliance Committee, and Vice Chair of the FRCC Critical Infrastructure Protection Committee. Rich is a Certified Information Systems Security Professional (CISSP) and Certified Ethical Hacker.

Rich is a graduate of the University of Central Florida with a Bachelor of Science in Electrical Engineering and a Master of Business Administration.

Barry Kuehnle

CIP Senior Advisor, Federal Energy Regulatory Commission, Office of Energy Infrastructure Security

Barry Kuehnle is a senior critical infrastructure protection advisor for the Office of Infrastructure Security (OEIS) at the Federal Energy Regulatory Commission. Barry's focus has been on cyber security, specializing in industrial control system security since the mid 90's. He started his security career with the Navy assigned to a cryptologic command. After the Navy, Barry worked at the Idaho National Laboratory in the Homeland Security Directorate within the Critical Infrastructure Protection Division.

Bill Lawrence

Manager of Critical Infrastructure Protection (CIP) Awareness, NERC

Bill Lawrence began at NERC in July 2012 in the Washington, D.C., office as the Manager of CIP Awareness. Prior to joining NERC, he most recently was the Deputy Director, Character Development & Training Division, at the United States Naval Academy, where he also taught courses in Ethics and Cyber Security. Bill flew F-14 Tomcats and F/A-18F Super Hornets for the Navy, and has a B.S. in Computer Science from the US Naval Academy. He has a Master of Science in International Relations from Auburn Montgomery, and a Master of Military Operational Art and Science from the Air Command and Staff College. Bill holds a Project Management Professional certification.

Paul McElroy

Managing Director and CEO, JEA

Mr. McElroy is Managing Director and Chief Executive Officer of JEA – Jacksonville, Florida's municipally owned electric, water and wastewater utility. The JEA Board of Directors named Paul the company's seventh Chief Executive Officer effective October 1, 2012. From January 1, 2006 to October 1, 2012, he served as JEA's Chief Financial Officer. Prior to that, he served as JEA's Vice President, Financial Services.

areas of electric system operations, nuclear and fossil plant operations, substations, and distribution. He served five years as an officer in the U.S. Army Corps of Engineers. Mr. Cauley holds a BS degree from the U.S. Military Academy at West Point, an MS degree from the University of Maryland in Nuclear Engineering, and an MBA from Loyola College - Baltimore. Mr. Cauley is a registered Professional Engineer in the Commonwealth of Virginia.

The Honorable Michael Chertoff

Co-founder and Managing Principal, The Chertoff Group

As Secretary of the U.S. Department of Homeland Security from 2005 to 2009, Mr. Chertoff led the country in blocking would-be terrorists from crossing our borders or implementing their plans if they were already in the country. He also transformed FEMA into an effective organization following Hurricane Katrina. His greatest successes have earned few headlines – because the important news is what didn't happen.

At Chertoff Group, Mr. Chertoff provides high-level strategic counsel to corporate and government leaders on a broad range of security issues, from risk identification and prevention to preparedness, response and recovery. "Risk management has become the CEO's concern," he says. "We help our clients develop comprehensive strategies to manage risk without building barriers that get in the way of carrying on their business."

Before heading up the Department of Homeland Security, Mr. Chertoff served as a federal judge on the U.S. Court of Appeals for the Third Circuit. Earlier, during more than a decade as a federal prosecutor, he investigated and prosecuted cases of political corruption, organized crime, corporate fraud and terrorism – including the investigation of the 9/11 terrorist attacks.

Mr. Chertoff is a magna cum laude graduate of Harvard College (1975) and Harvard Law School (1978). From 1979-1980 he served as a clerk to Supreme Court Justice William Brennan, Jr.

Dr. Michael L. Cohen

Principal Critical Infrastructure Systems Engineer, MITRE, Homeland Security Center

Dr. Cohen is considered a MITRE corporate resource in the area of critical infrastructure protection and resilience. Dr. Cohen helped to establish two vital national critical infrastructure institutions: the National Infrastructure Protection Center at the FBI and the Office of Infrastructure Protection at the Department of Homeland Security. Dr. Cohen's own critical infrastructure specialty is in the Energy Sector, more specifically concerning Electric Power, Smart Grid, Nuclear Power, and Oil & Natural Gas.

Most recently Dr. Cohen has been focusing on assessing and mitigating the risk to critical infrastructure from disruption of GPS position, navigation, and timing services. In parallel with and prior to that focus, Dr. Cohen has been supporting critical infrastructure Cybersecurity and supply chain risk management programs at DHS. Dr. Cohen earned his PhD at the University of Maryland, his Master's Degree in Physics at Northeastern University and his Bachelor's degree in Physics at Boston University.

Matt Davis

Ernst & Young

Matt Davis is a Manager in the Advisory Services practice of Ernst & Young LLP. He has over 10 years of experience in planning, designing, managing, and assisting enterprise-wide information security services, with focus on performing risk assessments and advising on information security strategy with a specialization in compliance and regulatory issues. Matt has been involved in engagements with clients across multiple domains including Financial Services, Power Utility, Retail, and Government.

Stephen Diebold

Senior Director Product Management, Advanced BI Solutions

Mr. Diebold is the Senior Director of Product Management over Ventyx's Advanced Business Intelligence Solutions. He is currently leading the initiative on Storm Damage Prediction and overseeing Ventyx and ABB participation in NERC's GridEx II. He has served on Southwest Power Pool Critical Infrastructure Protection Working Group, served as a representative on NERC's Critical Infrastructure Protection Committee (CIPC), and served on NERC's CIPC Cyber Attack Task Force. Mr. Diebold currently chairs NERC's CIPC Electricity Sector – Information Sharing Tasks Force. In 2007 He was awarded the SANS "National Cybersecurity Leadership Award" for his work as chairman of the ABB / Idaho National Lab / DOE / Customer Consortium on EMS cyber security research.

Mr. Diebold's 31 plus year career in the electric utility industry includes time spent in Power, Transmission, Distribution, and Information Technologies areas. He has published articles in Utility Automation T&D, Transmission and Distribution World, and Electric Light and Power magazines. He has served on and chaired several utility industry user groups and utility vendor customer advisory boards. Before assuming his current position, Mr. Diebold served as Manager of Real-time Systems for Kansas City Power and Light Company (KCPL) where his responsibilities include managing KCPL's Energy Management System, Transmission and Generation Energy Accounting System, Outage Management System, Distribution's business intelligence initiatives, Enterprise Asset Management, Enterprise Work Management, and Power Services Energy Trading Systems. Mr. Diebold has a Bachelor of Science degree in Electrical Engineering and a Master of Science in Electrical Engineering from the University of Missouri at Rolla. He is a member of the Institute of Electrical and Electronics Engineers, a registered Professional Engineer in Missouri and a registered Project Management Professional.

Mark Fabro

President and Chief Security Scientist, Lofty Perch

Mark Fabro is the President and Chief Security Scientist for Lofty Perch, Inc. a market leading security technology company focused on SCADA and control system cyber security. As a recognized expert in attack methodologies and adversarial techniques, his work is focused on threat modeling, incident investigations and counter-attack planning. His projects have included supporting some of the largest infrastructure asset owners in the world, and in addition to being involved in the development of several security standards for transportation, energy, and water sectors, he has testified to Congress on cyber security risk and threat to the North American Bulk Power System.

Mr. Fabro was a contributing specialist to the U.S. National Strategy to Secure Cyberspace, the Cyber Annex to the National Response Framework, the post-Katrina control systems recovery plan for Oil and Gas, and most recently the Department of Energy/White House Cybersecurity Capability Maturity Model. He has authored several of the Recommended Practices for the DHS Control Systems Security Program/Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), helped found the Repository for Industrial Security Incidents, and is a member of both the NERC Smart Grid and Cyber Attack Task Forces.

On the research side, he is well known for the discovery of numerous critical vulnerabilities in industrial automation technology, authoring early proof-of-concept code for ICS malware and is a contributing developer to numerous SCADA assessment frameworks. He is regularly published for his work on Smart Grid, integrated radio mesh communications, and control systems forensics. He is the co-founder of the SCADASEC mailing list, and is involved in several international working groups addressing 'denial of control' within the process control and SCADA domain.

Mr. Fabro has a degree in applied physics and mathematics and is currently working on his PhD in Electrical and Information Engineering. He has completed post graduate studies in national security and counterterrorism at both the American Military University and the United Nations, and has taught cyber security theory at several universities and government agencies around the globe. Recently, for his work in critical infrastructure protection, he was recognized as one of the '25 Most Influential Consultants in the World' and was named 'Information Security Professional of the Year' by SC Magazine.

Roger Fradenburgh

Principal Security Architect, Network & Security Technologies, Inc.

Mr. Fradenburgh has over 30 years of experience in communications and information security. Since joining Network & Security Technologies in 2005, he has focused almost exclusively on the electric utility industry and on CIP Standard compliance. He has worked with Responsible Entities in nearly all of the eight Regions on virtually all aspects of CIP compliance, from bootstrapping new compliance programs to maintaining and updating existing programs through activities such as Cyber Vulnerability Assessments, gap analyses, and mock audits.

Mr. Fradenburgh has taken NERC auditor training courses, and since 2009 has represented Responsible Entities, a Regional Entity, and NERC during NERC CIP audits.

Mr. Fradenburgh is a regular attendee at NERC CIPC meetings, and he was an active and contributing member of the Risk Assessment Working Group, which developed and published CIP-002-3 Critical Asset Identification and Critical Cyber Asset Identification guidelines. During 2010 and 2011, he served as an Observer Participant member of the Order 706 Standard Drafting Team, which developed Version 5 of the CIP Standards.

Mr. Fradenburgh is a Certified Information Systems Security Professional (CISSP) and is a graduate of Brown University.

Gregory Goodrich

Principal, Security and Compliance Coordination, New York Independent System Operator

Greg Goodrich is the New York Independent System Operator (NYISO) Principal, Security and Compliance Coordination. He has over 29 years experience working with industrial control systems (ICS), supervisory control systems and data acquisition systems (SCADA), energy management systems (EMS), security, and information technology and software. Currently he is serving as the chair of the NPCC Task Force on Information Security and Technology and is a NERC Critical Infrastructure Protection Committee (CIPC) representative. Greg also serves on the ISO/RTO Council (IRC) Security Working Group supporting cyber security, physical security, and compliance matters. Most recently he has been working in support of the Electric Sub-Sector activities following the Executive Order (EO 13636) and Presidential Policy Directive 21 (PPD-21) including the Integrated Task Force and the update to the National Infrastructure Protection Plan.

Greg joined the NYISO in 2001, where he supported and lead aspects of the Standard Market Design II (SMD-II) project and DOE Smart Grid Investment Grant project, managed Enterprise Security, and coordinated NYISO's NERC CIP compliance program. Additionally Greg worked for Vermont Electric Power Company for 12 years managing IT and SCADA/EMS groups. He holds several industry and security certifications including the Certified Information System Security Professional (CISSP).

Andrew Ginter

Vice President of Industrial Security, Waterfall Security Solutions

Andrew Ginter is the Vice President of Industrial Security at Waterfall Security Solutions. He spent the first part of his career developing systems-level and control system products for a number of vendors, including Honeywell and Hewlett-Packard. At Agilent Technologies, he led the development of middleware products connecting industrial control systems to the SAP enterprise resource planning system. As Chief Technology Officer at Industrial Defender, Andrew led the development of the core standards bodies and works with customers to incorporate Waterfall Unidirectional Gateways into their industrial network designs. Andrew holds degrees in Mathematics and Computer Science from the University of Calgary, as well as ISP, ITCP, and CISSP accreditations.

David Graham

Vice President, Owl Computing Technologies

Dave Graham is Vice President and minority owner of Owl Computing since 2000. He started his career at Arthur Andersen & Co. in its Energy and Telecommunications Practice, after completing his service in the U.S. Army. He has served as the Chief Financial Officer of a highly successful nationwide, multi-service utility, the Chairman and Chief Executive Officer of a publicly traded utility company and the President of several privately owned companies.

Dave holds a BS in Business Administration from the University of Missouri and received his MBA from the New York University Executive General Management Program. He is a Certified Public Accountant. He is a member of the Armed Forces Communications and Electronics Association, Association of the United States Army, Financial Executives International, and the American Institute of Certified Public Accountants, and has been affiliated with the Association for Corporate Growth, National Association of Corporate Directors, and the Connecticut Venture Group.