

# Industrial Control Cybersecurity USA 2015

Subject to change  
For opportunities contact:  
James Nesbitt, james.nesbitt@cybersenate.com  
+1 916 692 0184 USA

Copyright Cyber Senate 2015.

13th and 14th October 2015

Pre Conference Workshop 12th October

Hyatt Regency

Sacramento, California



## Our Sponsors

Headline Sponsors

**BAE SYSTEMS**

I N S P I R E D   W O R K

Co Sponsors



Sponsors



[www.industrialcontrolsecurityusa.com](http://www.industrialcontrolsecurityusa.com)

To register call +1 916 692 0184 or [marketing@sagacity-media.com](mailto:marketing@sagacity-media.com)

# THE GOAL OF THE CONFERENCE

---

All stakeholders have a new responsibility in ensuring the safety, reliability and stability of our Critical National Infrastructure. Public and Private partnerships are paramount and information sharing on an international level a priority. We will be addressing key areas of vulnerability, threat detection, mitigation, and planning for the Energy, Oil, Gas, Electric and Water Sectors.

The Industrial Control Cybersecurity conference consists of presentations and debate from some of the energy industry's leading end users from Operational and IT backgrounds, Government influencers, leading cybersecurity authorities and some of the world's most influential solution providers.

Key topics of discussion will pivot on convergence of operational and information technology transformation, design, implementation, integration and risks associated with enterprise facing architecture.

Further review includes the development of policy, operational and cultural considerations, maturity models, public and private information sharing and the adoption of cybersecurity controls.

2015 will provide further insight into how industry can further develop organisational priorities, effective methodologies, benchmark return on investment for cybersecurity procurement, supplier relationships and how to effectively deploy defense in-depth strategies.

We will introduce discussion on the latest attacks and hear from those who are responsible for identifying them. The conference will further address penetration testing, the art of detection and threat monitoring, incident response and recovery.

---

## Goals of the conference

The goal of the conference – to enhance dialogue and information sharing between public and private sectors, providing participants an opportunity to contribute and engage on some of our country's most pressing security threats surrounding critical national infrastructure. Our vision as a collective to enhance resilience and the adoption of cybersecurity controls within the Energy, Water, Oil, Gas, Electric, Chemical and Nuclear sector.

\*\*Copyright 2015 Sagacity Media Ltd.

## Why you cannot miss 2015

- Gain further understanding of the risks and opportunities created by the convergence of operational and information technology
- current areas of vulnerability, threat detection, mitigation, maturity capability models and risk management.
- Take away tools to assist in developing organisational priorities, methodologies and how to effectively deploy defense in-depth strategies.
- Hear how your industry counterparts are defining and benchmarking return on investment for cybersecurity procurement, supplier responsibilities and adapting new models for incident response.
- Take part and contribute to the technological transformation IT/OT shift involving design, implementation and integration requiring the collaborative efforts of two unique but historically different skillsets.

## Target Audience

The Industrial Control Cybersecurity Europe conference consists of presentations, debate and contribution from some of the energy industry's leading Chief Information Security Officers, Operational and IT Divisional Heads, Government influencers and world leading cybersecurity authorities and solution providers. Our focus is on providing a educational platform to enhance resiliency and public and private information sharing, with a heavy focus on end users and responsibility.

## The engineering art of injecting and managing Industrial Cyber Security within the entire life cycle of the control system

### Overview of Workshop

More than five years have passed after Stuxnet and the world realized the need to protect critical infrastructures from the emerging threats. We live in the era of cyber war, hacktivism, and building electronic armies. While we talk a lot about industrial cyber problems there is a need to talk more about effective practical solutions. The workshop will highlight the importance of understanding the combination of the industrial cyber security, automation, and understanding plant production models in order to design the right cyber secure infrastructure and solutions. The session will also cover the important aspects that need to be addressed by the stakeholders to achieve the goals. Ayman will focus on covering a comprehensive overview of the practical approach for designing, injecting and implementing cyber security for the Industrial Control Systems from Front End Engineering Design (FEED) Stage to the EPC (Engineering, Procurement and Construction).

### Why you should attend

Why we have to properly understand the plan operation when designing cyber security models and solutions for control systems  
Learn how to embed industrial cyber security technical assurance in project lifecycle  
Discuss the different types of critical infrastructures (energy, utilities, etc.) and how the type of operation is related to cyber security  
Develop ideas on how to move into cyber security by design for the new control systems.  
Understand how to enhance industrial cyber security within existing control systems  
What you need to address before implementing cyber security solutions in the existing ICS systems

### Program

9.00 Registration & coffee  
10.00 Session 1  
11.45 Break  
12.30 Session 2  
15.00 End of workshop

### Workshop main bullets

- Understanding the emerging cyber threats
- Discuss the latest ICS reports and incidents including the lessons that shall be learned
- Need for different industrial cyber security models for the different critical infrastructure
- Who are the stakeholders and what is the role of each?
- What are the important three C's for effective cyber security?
- Why do we need to understand plant operation when planning to secure the plants from cyber threats?
- What are the pre-requisites that you must consider before implementing industrial cyber security?
- How to engineer and enhance cyber security for an old plant?
- Implementing Industrial Cyber Security by Design for the new plant or new automation system upgrades
- Understanding the ISA99/IEC62443, and understanding the SILs and SALs
- Why the Security Operation Center is must?
- Impeding cyber security within the automation system/project life cycle

### About the Workshop

#### Host

Ayman AL-Issa, Chief Technologist,  
Industrial Cyber Security, Booz Allen Hamilton



Ayman has over 22 years of experience in the fields of Automation, Information

Technology, and Cyber Security. He has graduated with a Bachelor's degree in Electronics Engineering in 1992 and verse in different backgrounds like industrial control systems, systems engineering, and building cyber security strategies and models. He is a member in the Cyber Security Advisory boards of top rated worldwide universities for the advancement of researches on industrial cyber security. He is an active member in different international Security Innovation Alliances that are focused in a worldwide program for improving the security of industrial control systems by the close collaboration of the leading IT Security and industrial control system vendors. He is also information contributor to the ISA99/IEC62443 Industrial Automation and Control Systems Cyber Security Standards, and he is currently leading workgroup 1 in the standard. Realizing that security measures are always behind the emerging cyber risks, he developed an ICS defense-in-depth industrial cyber security model that aims to early detection of threats based on security-through-vision-and-integration. Ayman worked for ADMA-OPCO for 17 years and he was the Digital Oil Fields Cyber Security Advisor. He joined Booz Allen Hamilton in 2014 as the Chief Technologist & Senior Advisor/Architect in Industrial Cyber Security – MENA.

## Headline Sponsors

# BAE SYSTEMS

## I N S P I R E D   W O R K

As 2014 drew to a close, more details began to emerge about a reported spate of attacks against companies in Norway's oil and gas industry. According to reports, at least 50 companies were hacked, and a further 250 were warned of the risk by the nation's prevention unit for cyber attack – National Security Authority (NSM). Although it would appear that no industrial operations were directly impacted, this attack has once again raised the concern of what the impact of a larger, well-planned attack could be if targeted against Critical National Infrastructures (CNI) and leading industries. The concern is a valid one: security experts are worried that many of the industrial processes that power our modern lives may be vulnerable to cyber attack, because the necessary levels of layered security that have over the years been put in place to protect our information technology (IT) and keep business running, have not yet been fully deployed to protect the Operational Technology (OT) that makes our industries work. This is because historically, industrial processes and the technology that supports their operation, have been isolated from the outside world. However, increasingly, industrial processes, utilities and factories are becoming IP enabled and interconnected with each other and their Corporate/IT networks, exposing them to risks and dangers that were never considered in their original design: the threat of malware and cyber attack. As a company that delivers solutions to government and commercial customers to help secure the CNI, we at BAE Systems Applied Intelligence value the opportunity to participate in the ICS Cyber Security Conference. It creates an environment in which we can continue learning about the latest challenges our clients are facing as well as providing the opportunity to discuss our views on security best practices.

### Colin McKinty

Vice President of Cyber Security Strategy, Americas

**BAE Systems Applied Intelligence**



Zscaler protects 12 million employees at 5,000 organizations worldwide against cyberattacks and data breaches. Zscaler's Security-as-a-Service platform delivers Internet security, APT protection, data loss prevention, SSL decryption, traffic shaping, policy management and threat intelligence, ensuring a safe and productive Internet experience for every user, from any device and any location.

[www.zscaler.com](http://www.zscaler.com)



As a leader in industrial controls, GE is committed to assist critical infrastructure owners in improving their security postures and supporting compliance efforts. GE's approach includes adapting cyber security to fit unique industrial architecture and business requirements, employing the latest technology and knowledge in cyber threat management, and giving proven recommendations for operational security improvement.

<http://www.ge-mcs.com/en/cyber-security.html>



Codonomicon provides a suite of next-generation solutions that reveal a better path to total defense. These solutions provide new layers of testing, robustness, intelligence, collaboration and security to deliver strength in visibility to the very Core of today's critical systems, networks and devices. Founded in 2001 in Oulu, Finland, the global company works with leading telecommunications, networking, manufacturing, healthcare, financial services, defense, government, CERT and cyber authorities to strengthen systems and proactively secure customers and connections.

[www.codenomicon.com](http://www.codenomicon.com)



- 09:10am - 10:10am **Keynote Presentation Department of Homeland Security**  
 (\*suggested presentation topics, final confirmation of bullets posted shortly)  
 Industry transformation and public and private information sharing initiatives  
 What are we doing collectively to mitigate the potential risk, what barriers are we experiencing and how are we transforming as an industry to put strategies in place?  
**Marty Edwards**, Director Industrial Control Systems Cyber Emergency Response Team (ICS-CERT),  
**Department of Homeland Security**
- 10:10am - 10:50am **Compliance and the foundation of risk control**  
 Foundation Surge information sharing  
 Nation State activities  
**Tim Roxey**, Chief Security Officer Senior Director, **NERC**
- 10:50am - 11:20am **Coffee and Exhibitor Networking**
- 11:20am - 11:50am **Industrial Control Cyber Security Opportunities on a State-Wide Level**  
 What the CIO and CISO Need to Know and Respect About ICS and CI  
 NIST Special Publication 800-82 relationship with NIST 800-53 Rev. 4 Controls  
 Who Has ICS and CI Responsibility In Organizations?  
 Public and Private Information Sharing Opportunities on a State-Wide Level – Build Relationships  
 Professional Perspective – How Can IT Policy and Procedure Converge with ICS Service Level Perfection?  
**Mary DiPietro**, Deputy Chief Information Security Officer, California Department of Technology, **California Information Security Office**
- 11:50am - 12:20pm **Panel: Coordinated approaches between Government and State**  
**Audience Q&A**  
**Marty Edwards**, Department of Homeland Security, **ICS CERT Director**  
**Tim Roxey**, Chief Security Officer Senior Director, **NERC**  
**Mary DiPietro**, Deputy Chief Information Security Officer, California Department of Technology, **California Information Security Office**
- 12:20am - 1:00pm **A vision from our Headline Sponsors**  
  
 I N S P I R E D W O R K
- 1:00pm - 2:30pm **Lunch and Networking**   
**Sponsored by GE**
- 2:00pm - 2:30pm **What Iberdrola learned as we developed our framework for cyber security risk management, which we are implementing around the world**  
 Approach, methodologies, lessons learned from this global effort  
 Steps to assess current levels of cyber security  
 Identifying risk for each business, cataloguing best practice  
 Developing risk maps and customised implementation plans  
 The systemized approach helped us provide clear direction and guidance, establish reliable and repeatable process, and communicate cyber security risks more effectively.  
**Keri Glitch**, Vice President Corporate Security, **Iberdrola USA**
- 2:30pm - 3:00pm **Maturing SCADA Security Programs**  
 Establishing and maturing an ICS/SCADA security program  
 Business, security, and compliance drivers  
 Special considerations and challenges to achieve  
 Example of utility approaches  
**Samara Moore**, Senior Manager, **CIP Security & Compliance, Corporate and Information Security Services, Exelon**
- 3:00pm - 3:30pm **Exhibitor Networking**

3:30pm - 4:10pm

**Managing Software Security Throughout The Supply Chain**

All businesses rely on both a domestic and an international supply chain on a daily basis, as such we rely on software security throughout the entire supply chain and this is where things become challenging. The software industry relies on third party open source code as part of their internal systems, as well as a rapidly increasing number of third party commercial offerings. A major cybersecurity vulnerability discovered in a commonly used third party software component can lead to massive challenges resolving the issues. (Heartbleed/Shellshock)

Reliance on vulnerable third party components require organisations to revisit their cybersecurity management strategies and security audits.

Organisations are frequently hesitant to impose requirements for managing cybersecurity on those outside of their organisation.

We are not dealing with technological problems as much as we are dealing with policy problems

**Mike Ahmadi**, Global Business Development Director, **Codenomicon**



4:10pm - 4:50pm

**Integrated Control and Safety Systems**

Looking at industrial cyber security from a safety perspective will enable us to design safe secure cyber solutions. The session will focus on understanding the relation between system safety and cyber security and will touch on the ICSS "Integrated Control and Safety Systems". The session will also discuss the importance of segregating safety and control systems from cyber secure perspectives?

- Understanding the relation between safety and security
- Visualizing TUV certified systems and Cyber Security
- Addressing cyber security needs for the ICSS.

**Ayman Al Issa**, Chief Technologist & Senior Advisor, Industrial Cyber Security, **Booz Allen Hamilton**

4:50pm - 5:30pm

**Industrial Cyber Security; is it a test-tube baby?** After more than 5 years of Stuxnet, we need to admit that the mature industrial cyber security baby has not been born yet. This session is covering a transparent discussion on the status of industrial cyber security today and how it is much behind the emerging threats. Who are the stakeholders and are they doing what they should do? Is it a complicated situation that needs a complex approach? How can we get things moving ahead?

**Panel led by**

**Ayman Al Issa**, Chief Technologist & Senior Advisor, **Industrial Cyber Security**, **Booz Allen Hamilton**

**Includes Panellists:**

**Samara Moore**, Senior Manager, CIP Security & Compliance, Corporate and Information Security Services, **Exelon**

**Keri Glitch**, Vice President Corporate Security, **Iberdrola USA**

**Mike Ahmadi**, Global Business Development Director, **Codenomicon**

**Invited: Marty Edwards**, Director Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), **Department of Homeland Security**

**Invited: Tim Roxey**, Chief Security Officer Senior Director, **NERC**

5:30pm - 6:00pm

**BAE Systems Applied Intelligence roundtable and more to be announced**

6:00pm - 7:00pm

**Drinks reception sponsored by BAE Systems Applied Intelligence**

- 09:10am - 9:40am **Key Note ICS ISAC  
ICS Security Lifecycle**  
**Chris Blask, Chair at Industrial Control System Information Sharing and Analysis Center**
- 09:40am - 10:10am **Case Study: The 2012 cyber-attacks against Saudi Aramco and the Aramco family of affiliates was a major game changer in IT & ICS Security.** The energy sector, relevant markets and governments worldwide shuddered. Although oil production wasn't directly affected, business operations were greatly interrupted and remain so. This presentation is the story how I implemented the first IT Security unit for Aramco Overseas Company, a Saudi Aramco affiliate which provides all IT services for Saudi Aramco in South America and the EMEA region outside of Saudi Arabia.
- 1.Cybergeddon 2012**
- Description of Shamoon and attack effects on the Aramco family
- 2.Starting from Zero to Hero**
- An offer I couldn't refuse after "The Incident"
  - Implementation of basic IT security
  - Recruitment of skilled in-house IT security staff
- 3.Maturation -IT Security to the next level**
- Development of staff: hackers, lock pickers, geniuses and Harlem Shakers
  - Exercises and independent operational audits
  - Building the framework for a functional incident response team and CERT
- 4.Lessons Learned**
- Twitter setbacks
  - Dealing with panic
  - What I would do different if I had a time machine
- Chris Kubecka, Former Head of Operations Centre, Aramco Overseas,  
Researcher Security Evangelist EU**
- 10:10am - 10:40am **Governance, Incident response and recovery**  
Governance structure  
Risk advisory and strategic direction  
Governance on security operations  
Standardisation and compliance  
Defining and implementing a process  
Monitoring and detection  
Incident management: Incident, incident response, incident investigation  
**Scott King, Manager Information Security, Sempra Utilities**
- 10:40am - 11:10am **Exhibitor Networking**
- 11:10am - 11:40am **Compliance Doesn't Equal Security – but They're Not Mutually Exclusive:**  
How to obtain synergy by architecting security solutions which can deliver compliance.  
Key Points / Themes:
- \* This statement is pervasive – all security practitioners echo it. How can we change this?
  - \* Holistic security architecture must span physical, OT, IT, and varying LoB priorities
  - \* Knowing key control points and artifacts, technology and process for generating compliance evidence can be "baked in" rather than "bolted on".
  - \* Compliance represents the 'minimum criteria', and closely align to security best practice (e.g. SANS Top 20 Security Controls).
  - \* Opportunities to go above and beyond: OT Networks are less dynamic than corporate networks – offering a better opportunity for baseline modeling, and anomaly detection
- Billy Glenn, Principal Architect, PG&E**
- 11:40am - 12:10pm **Panel: Defining a risk, compliance and governance framework that integrates IT and OT security – Best Practice**  
Evaluating business IT and OT performance through operational dashboards  
Key policies, definition of corporate control for each sector  
Managing operational and IT high risk areas- Long term thinking  
Developing a streamlined process of managing compliance and managing cost
- Chris Blask, Chair at Industrial Control System Information Sharing and Analysis Center (ICS ISAC)  
Christina Kubecka, Private Researcher, SecurityEvangelistEU, Former Group Leader, Aramco Overseas The Netherlands  
Scott King, Manager Information Security, Sempra Utilities  
Billy Glenn, Principal Architect, PG&E**

12:10pm - 12:40pm **Defending Against Cloud-Originated Threats**

Why does fighting cloud-based threats in the cloud make sense for industrial IoT and why is it proving more effective than traditional security architectures?

How does cloud-based security work and how does it secure specific vulnerabilities found in Internet-facing ICS/Scada?

The adoption of cloud computing is inevitable for critical environments, how can we enable that adoption and assure the industry that it's a safe way forward for critical infrastructure?

What are current trends in the threat landscape (drawn from over 15 billion transactions processed daily)?

What are expected future developments in cloud-based security?

**Patrick Foxhoven**, VP & CTO of Emerging Technologies, **Zscaler**

12:40pm - 1:40pm **Lunch and Networking**1:40pm - 2:10pm **ICS threat categorization and indicators of compromise**

Automatic machine-response to ICS threats

Threat sharing best practices

**Doug Rhoades**, Chief Engineer for Cybersecurity, **Southern California Edison**

2:10pm - 2:40pm **Integration of Operations Data and Command and Control messages to ensure cyber security and power system resilience.**

CWP is building operational tools that integrate PMU measured power flow data, DNP3 SCADA messaging, and system power models to ensure that the grid is operating as expected and in a known state at all times. Abnormal power flows with related SCADA commands may be operator error or cyber actors. This system will detect events and potentially be able to reverse the attack and maintain power stability in future versions.

– Power system operations models

– SCADA command, control and data acquisition data

– Phase measurement units

– to provide a normal system awareness model for the entire power system

**Steven Brunasso**, Manager of Cyber Security, **California Water and Power**

2:40pm - 3:10pm **Culture Change; It's All About Security**

- Will examine both technical and human considerations

- Does your culture embrace security?

- Does your technical competence match today's environment of vulnerability?

**Glenn Steiger**, General Manager, **Alameda Municipal Power**

3:10pm - 3:40pm **Coffee and Exhibitor Networking**3:40pm - 4:10pm **Managing change in ICS environments, can modern security policies work in the ICS environment?**

Developing a culture of systemic thinking from an operations perspective and a IT perspective

Balancing the transformation of Mobility, Cloud, OT / ICS

System Awareness initiatives, implementation and development who are the key stakeholders and how do we engage

**Steven Brunasso**, Manager of Cyber Security, **California Water and Power**

**Doug Rhoades**, Chief Engineer for Cybersecurity, **Southern California Edison**

**Billy Glenn**, Principal Architect, **PG&E**

4:10pm - 5:30pm **What have we learned and what can we take away? Audience Discussion and Key Take Aways**

**End of Conference.** Presentation downloads will be made available to participants by the Cyber Senate with the permission of our speakers



## Marty Edwards

Director Industrial Control Systems Cyber Emergency Response Team, U.S. Department of Homeland Security Marty Edwards is the Director of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), an operational division of the department's National Cybersecurity and Communications Integration Center (NCCIC) and the DHS Office of Cybersecurity and Communications (CS&C).



## Keri Glitch

Vice President - Corporate Security, Iberdrola USA  
Keri Glitch is Vice President, Cyber and Physical Security for Iberdrola USA. In this role, Keri is responsible for creating an integrated, and standardized, security system for physical and cyber employees as well as our operations in 24 states from New England to the West Coast, which provide electricity generation, transmission & distribution, natural gas storage & distribution, and energy services. Keri recently attended the White House Summit on Cybersecurity and Consumer Protection – the invitation-only summit held at Stanford University in California. on Friday, February 13, 2015.



## Tim Roxey

Chief Security Officer  
Senior Director, 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) activities.



## Ayman Al Issa

Ayman AL-Issa, Chief Technologist – Industrial Cyber Security, Booz Allen Hamilton  
Ayman has over 22 years of experience in the fields of Automation, Information Technology, and Cyber Security. He has graduated with a Bachelor's degree in Electronics Engineering in 1992 and verse in different backgrounds like industrial control systems, systems engineering, and building cyber security strategies and models. He is a member in the Cyber Security Advisory boards of top rated worldwide universities for the advancement of researches on industrial cyber security.



## Chris Kubecka

Security Evangelist EU, Private Researcher, Group Leader, Chris Kubecka, Security Evangelist EU, Private Researcher, Former Group Leader, Aramco Overseas The Netherlands. Chris led the Security Operations Centre for Aramco Overseas Company. She holds degrees in Aeronautical Engineering, Computer Science and Information Technology. General Manager,



## Rene Moreda

Director of Business Development, Energy & Utilities, BAE Systems Applied Intelligence Mr. Moreda has over 20 years of experience developing, marketing and selling advanced technologies and solutions into the High Tech and Energy sector.



## Glenn Stieger

Alameda Municipal Power  
An accomplished, experienced and internationally recognized energy/water industry CEO-level leader. An effective strategist with broad knowledge of the energy business and over 30 years in leadership positions.



## Doug Rhoades

Cybersecurity GM and Chief Engineer , Southern California Edison  
Doug Rhoades is the Chief Engineer for Cybersecurity at Edison with responsibility for Incident Response, Tools and Engineering, Legislative Outreach, Threat Analysis and Remediation and Policy Development.



## Steven Brunasso

Manager Cyber Security, California Water and Power Utility  
He has focused on utility systems security for the past decade as the information security manager at Southern California Edison for the initial NERC CIP rollouts and is currently managing security in the operations technology group at one of the most innovative California Water and Power Utilities. He has an MBA from the University of California at Los Angeles specializing in technology strategy.



## Billy Glenn

Principal Enterprise Architect, PG&E  
Operational Technology focused security professional of PG&E's various SCADA, DCS, and other Industrial Control Systems. Billy was in the US Navy prior to joining Pacific Gas and Electric Company. A 22 year veteran of IT, Billy has strived to always be learning, working in a variety of evolutionary areas: from telecommunications, the creation of enterprise networks, migration from the mainframe to client/server, and over a decade as Internet architect designing and implementing Internet, Intranet and B2B technologies from simple logo-ware to fully-interactive customer self-service portals.



## Mike Ahmadi

Global Director of Critical Systems Security , Codenomicon, Mike Ahmadi is the Global Director of Critical Systems Security for Codenomicon Ltd. Mike is well known in the field of critical infrastructure security, including industrial control systems and health care systems. He currently serves on the technical steering committee for the ISA Security Compliance Institute (ISCI) who manages and maintains the ISASecure certification program. Mike also currently serves as an active member of the US Department of Homeland Security Industrial Control Systems Joint Working Group, and as part of the advisory board for the US Secret Service Electronic Crimes Task Force



## Scott King

Mr. King started his career as a network and systems engineer in the mid 1990's. In early 2001 he moved into the information security field supporting the Department of Defense. Over the past 10+ years Mr. King has held multiple roles within the security community supporting federal government and state government, DoD, commercial companies, and most recently critical infrastructure. For the past six years, Mr. King has worked for the Sempra Energy family of companies in multiple security roles. Today Mr. King is responsible for managing the cyber security department for all utility IT and critical infrastructure supporting SDG&E, Southern California Gas, and the parent company Sempra Energy.



## Mary DiPietro

Mary joined the CISO as Deputy Chief in January 2014 from her position as Director of Information Technology for the State of Connecticut, Department of Developmental Services. In her role as Deputy CISO, Mary participates in initiatives to review and include state information security policy compliance throughout project lifecycles and consults with agencies on best practices for compliance implementation. DiPietro has technical project management experience with secure networks, web application development, configuration management, encryption, customer service and information security auditing. She implemented the HIPAA technical controls at the State of Connecticut, Department of Mental Health and Addiction Services, and was responsible for developing security awareness and training for business and technical audiences. Mary's early career at the Department of Information Services, City of Hartford, Connecticut gave her a foundation in systems programming and operations management where she gained experience with data center disaster recovery and technology restoration. Mary is a Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), and Certified Information Security Manager (CISM).



## Samara Moore

As a Senior Manager for CIP Security and Compliance within Exelon Corporate Information Security Services, Moore focuses on partnering across the enterprise to manage cyber and physical security and compliance along with the ICS/SCADA Security Program. Mrs. Moore joined Exelon after spending the last 10 years in the federal government in various roles. While serving in the government, she was a member of the White House National Security Council Staff, where she was the Director for Cybersecurity Critical Infrastructure Protection coordinating across the federal government and partnering with the private sector on information sharing, capability development and executive engagement efforts to strengthen cybersecurity for all critical infrastructure sectors. At the Department of Energy (DOE), Samara Moore was responsible for the cyber policy and oversight for the programs within the Office of the Under Secretary for Science and Energy, and held leadership roles supporting security and resilience for the Energy sector. While at DOE, Mrs. Moore also led the development of the Electricity Sector Cybersecurity Capability Maturity Model which is being used both domestically and internationally. Prior to her government service, she worked as an enterprise risk and security consultant. Mrs. Moore is a graduate of Virginia Tech with a B.S. in Accounting & Information Systems, and a graduate of George Washington University with a M.S. in Systems management/Information Security



## Patrick Foxhoven

Patrick Foxhoven is an experienced and innovative managed security entrepreneur and technologist, having spent 20 years building secure and scalable Internet-enabled networks while co-authoring three books on information security and receiving multiple patents. He is currently Vice President and Chief Technology Officer of Emerging Technologies at Zscaler, having served previously as Vice President of Cloud Operations, where he was responsible for the global deployment and operations of the world's largest security cloud, with an infrastructure spanning 100+ data centers processing Internet traffic from enterprise customers in 180+ countries. Prior to joining Zscaler in 2010, he was a founder and CIO of CentraComm, a leading managed IT security and services provider, and served earlier as the Vice President of a Midwest-based ISP.

