Call for Speakers/Panelists

15th Annual EnergySec Security and Compliance Summit

Planning has begun for this year's EnergySec Summit and we are pleased to open the Call for Speakers for this event. We are seeking at least 60 speakers, panelists, and moderators to fill 30 hours of educational and information sharing time across three days. Opportunities exist for plenary session panels and presentations on days 2 and 3, plus focused breakout sessions on day 1.

We are looking for knowledgeable people who can passionately and effectively share their subject matter expertise, real life experiences, solutions, and concerns with attendees of our 15th Annual Security & Compliance Summit, August 19-21, 2019, at the Disneyland Hotel in Anaheim, CA.

Speaking Proposals should be emailed to: cfs@energysec.org no later than April 15, 2019. We expect to make selections by May 15, 2019.

Please include the following information in your submission:

- Full Name
- Speaker name (if different than submitter)
- Email Address
- Company/Organization
- Job Title
- Short Biography
- Topic, Panel, or Breakout Session of interest
- Title and Abstract for presentation (if applicable)
- Time allotment desired (if applicable)

All submissions will be carefully considered, but preference is given to speakers currently employed at energy industry asset owners. Speaking opportunities exist in three general categories as listed below:

Plenary Session Panels (Days 2-3)

A moderator along with 3 panelists will examine and discuss an issue related to security or compliance in the energy sector. Panel topics will be determined as part of this Call for Speakers. Submitters may propose a complete panel package (topic, moderator, and panelists), a panel topic only, or simply request placement on an appropriate panel based on their background and experience.

Plenary Session Presentations (Days 2-3)

We have several 30-minute speaking opportunities available for presentations related to security or compliance in the energy sector. We welcome submittals from any interested party, but note that presentations designed primarily to promote a company's services, capabilities, or products will not be approved via the Call for Speakers. However, a limited number of sponsored speaking slots are available.

Breakout Sessions (Day 1)

Breakout sessions are designed to provide a deeper look at issues in one of four areas of focus. Session presentations of the following types are desired:

Lightning Talks (15 minutes)
Lightning talks are a great option for first-time or less experienced speakers. Gain experience and confidence in a small group session while sharing valuable information with your peers. These are also a great way to share quick-hit tips or lessons learned in your day-to-day work.

Presentations (30-60 minutes)
Full-length presentations provide more detailed discussions on relevant topics in any of the four tracks listed below.

Workshops (60-90 minutes)
Workshops provide time for a deeper and more interactive treatment of key issues. These are facilitated, interactive discussions on problems, challenges, or proposed solutions.

Topics of Interest

We will consider a broad range of topics relevant to cyber security in the energy sector. The topics below are of particular interest, but we will entertain other compelling proposals as well.

Risk Management: How are entities prioritizing security projects and expenditures to ensure the proper focus and level of security across the enterprise?

Emerging Risks: What new threats, vulnerabilities, or technologies should utilities be considering with respect to security?

Compliance and the Cloud: With multiple efforts in progress to address the clash of CIP compliance and cloud tech, what do utilities need to know to ensure security and compliance?

Supply Chain: With less than a year to go before mandatory supply chain standards go into effect for NERC CIP environments, and escalating concerns for cyber security risks from suppliers, what are utilities doing to address the issue?

ICS Security: The venture capitalists have spoken. ICS security companies now offer a plethora of products for securing industrial control environments. What types of technologies are being adopted and in what scenarios? (Note: This will be product neutral)

Information Sharing - Are we there yet?: Have we made any progress on this perennial buzzword? What’s new and promising on this challenging topic?

Rise of the Machines: Artificial Intelligence, Machine Learning, Big Data, Security Automation, and more. Are smarter systems supporting security schemes or will it all come back to bite us?

Security at the Edge: How is the proliferation of technology at the edge of the grid increasing cyber risk, and what should we be doing about it?

Hold my Beer: Lessons learned from projects or experiments gone wrong.

The Next Big Thing: What new technologies and techniques for cybersecurity offense or defense are tipping the scales?

That'll do: Case studies on security and compliance. What tools, technologies, or techniques are making a positive difference in security?

Right of Boom: Briefings on findings and lessons learned from security incidents within the industry.

My Kingdom for an Analyst: What's being done to grow the security workforce and strengthen the skills of current industry professionals?

Breakout Session Tracks

Security Leadership
This track is designed for security leadership. Topics may include risk management and planning, emerging threats, workforce development issues and solutions, security funding, governance, interacting with senior management, regulatory issues, and related items.

Security Operations
This session is focused on security operations. Topics may include security event monitoring, incident response, forensics, access administration, configuration monitoring, and similar topics.

Security Technology and Architecture
This session is focused on technical and architectural issues related to security. Topics may include the use of the cloud, new risks with grid modernization, defending against emerging threats and attack techniques, new technology, tools, or practices, security automation, and similar items

Compliance
This session is focused on regulatory compliance issues. Topics may include a range of NERC CIP areas including the new incident reporting requirements, supply chain standards, audit experiences, cloud and virtualization issues, guidance, compliance management tools and techniques, program case studies, new and modified standards in progress, state-level regulation, and similar items.