ENERGYSEC
SECURING CRITICAL INFRASTRUCTURE

Energy Sector Security Consortium, Inc.
8440 SE Sunnybrook Blvd., Ste. 206
Clackamas, OR 97015
877-2-NRGSEC (877-267-4732)
www.EnergySec.org

Request For Proposals
EnergySec Education Week Events 2019

Issued: November 26, 2018
Response Deadline: Open ended, but preference given to proposals received prior to Dec 31, 2018.

This Request for Proposals has been released by EnergySec to solicit potential training and instructors for its Education Week events in 2019 and beyond. EnergySec reserves the right to accept or reject any proposal. Proposals that fit with the purpose and objectives of this event, meet our content needs, and are financially feasible will be considered for formal agreements.

About Education Week
EnergySec Education Week events are designed to advance the cybersecurity skillset in the energy industry. The events are tuition-based, with attendance fees covering most or all of the associated costs. These events run from Monday morning through early afternoon on Friday, and are held at various locations across the U.S. To encourage networking and grow relationships within industry, lunch and dinner are typically provided and evening social events are planned and included in the cost of attendance.

Although no sponsorships are available, product and service providers are encouraged to submit proposals for educational sessions. Selections are based primarily on relevance and usefulness to the learning objectives established by EnergySec with financial considerations playing a secondary role. EnergySec Commercial Members are given preference where other factors are similar between submissions.

About EnergySec
The Energy Sector Security Consortium, Inc. (EnergySec) is a United States 501(c)(3) non-profit organization formed to support energy sector organizations with the security of their critical technology infrastructures. We support collaborative initiatives and projects, organize educational events and conferences, and provide informational products to our organizational members. EnergySec was established in 2002 and incorporated in 2008. Our members represent all segments of industry and all regions of the United States.

General Provisions

EnergySec reserves the right to reject any or all submitted proposals.

Submitted proposals should reflect course materials, instructors, and cost structures which the proposer is prepared to provide at any point in 2019. Proposals are not binding. If selected, EnergySec will negotiate formal agreements for one or more events to be held in 2019. Final terms and pricing may vary slightly from proposed amounts. Proposer may decline to participate in any or all events based on timing, location, staff availability, financial, or other reasons.

Dates and Locations
The following Education Weeks are currently planned for 2019:

Charlotte, NC | April 30 - May 3
Austin, TX | June 3-7
Colorado Springs | Late Sep or Early Oct

Topic Tracks
Each Education Week will contain one or more topic tracks around which courses will be selected and organized. Possible tracks are:

Industry Knowledge
This track is designed for industry security professionals that need a deeper understanding of how the industry operates, including specific technologies. This includes overall understanding of electric transmission operations and technology, power generation operations and technology, markets, distribution operations and technologies, communication technologies, protection systems, distribution automation, smart grids, advanced metering, and similar topics.

The ideal course in this track will explain how cybersecurity relates to operations and the underlying technologies, including potential avenues for attack, potential impacts, and possible risk mitigation strategies.

Hands-on Defense
This track is intended to provide hands-on, technical instruction of defensive practices for energy industry operations. This can include system baselining and hardening, security tool configuration and use, applying architectural principles and best practices to utility systems, practical application of frameworks.

Although commercial products may serve as a platform from which to teach, sessions in this category must provide conceptual knowledge that can be applied to any toolset in a given category. Product specific sessions will generally not be accepted for this track.

Security Operations
This track is designed for industry professionals in operational security roles, including event analysis, networking monitoring, threat hunting, security intelligence, incident response, and related areas. Ideal courses will provide detailed approaches and hands-on experience in these areas including, response exercises, red/blue team exercises, protocol analysis and related tools, threat hunting techniques, information sharing practices, tools, and systems, current threat intelligence updates, forensic and investigation techniques and tools, and related topics.

Tools and Demonstrations
In some cases, EnergySec may provide space for hands-on demonstration and learning of specific security related tools. EnergySec Commercial Members receive priority for any available space of this nature. Tools and Demonstration tracks are intended to be supplemental to primary tracks, and provide alternative sessions for attendees with interests in specific technologies. Sessions generally run 2 hours, and may be offered more than once at an event.

Course Content and Duration
The minimum desired course length is two hours. Courses of two or four hours, full-day, or two days will be considered. The ideal course will have an established curriculum which may include printed material and/or prepared slides. Proposals should include a description of the nature and extent of the established curriculum that will be used, including what will be

provided to students in hard copy and/or electronic formats. Courses may also rely on published textbooks or similar publicly available material.

An ideal proposal will include a course syllabus and learning objectives. Proposals should describe whether quizzes or exams are included as part of the course and any hands-on demonstrations or exercises.

2-hour courses
A typical 2-hour course will provide instruction on a focused topic relevant to the track objectives. Examples of previous 2-hour sessions include:

Jumping Airgaps
This course will discuss techniques for jumping across network airgaps. Learn how attackers operate and better defend your networks.

Threat Hunting Lab
In this lab, students will gain hands-on experience identifying attacks through the use of modern security tools.

4-hour courses (half-day)
A typical 4-hour course will provide more in-depth instruction on a focused topic. Examples of previous 4-hour sessions include:

Threat Hunting in ICS
In this course, students will learn techniques for identifying cyber attacks in ICS environments

Network Packet Analysis using Wireshark
Laptop required. In this half day course, students will learn the fundamentals of network traffic analysis using Wireshark, the de facto standard in packet analysis. Packet captures will be provided.

Full day or 2-day courses
Extended length courses provide an in-depth treatment of a broader topic area. These include topics that require extensive foundational or background information and often include hands-on exercises, labs, or demonstrations. Examples of extended length courses previously offered include:

Introduction to Network Threat Hunting for Utilities (8 hours)
This session will instruct students on theoretical and practical concepts which facilitate the creation of network threat hunting operations in utilities.

Applying the CIS Top 20 Controls in OT environments
This full-day course provides an overview of the Center for Internet Security's Top 20 Critical Security Controls, their applicability to Industrial Control System environments, along with tips and recommendations for deploying these types of solutions in highly sensitive environments.

Introduction to Security Assessments
In this course, students will learn the fundamentals of technical security assessments and become familiar with several common tools utilized for such work.

Instructors
Proposals should identify specific individuals that would be teaching the course, including biographical information, credentials, and work experience that demonstrates the qualifications necessary to teach the course. Multiple instructors may be proposed. Instructor assignments will be finalized upon execution of a formal agreement in conjunction with one or more events.

Cost Proposal
Proposals should identify any and all fees or expenses that will be charged for delivery of the course. Travel expenses may be listed by type and do not need exact estimates. EnergySec will typically directly pay lodging expenses for instructors on our master account for the event. Other expenses may be stated by type, for example, "round-trip coach airfare". Instructors are invited to participate in meals provided at the event, and separate reimbursement for those meals is typically not provided.

Cost proposals may be made in various forms. A common model is a flat rate for the instruction of the course, plus necessary expenses. An alternative is to propose a per-student rate, plus expenses, possibly subject to a minimum fee. Some organizations have charged for travel costs only. Tools and demonstrations are typically provided at no cost as an industry outreach practice.

Cost proposals will be a key determining factor after screening for relevance and usefulness of the proposed course.

Experience
Proposals should include a description of the experience of the organization and/or instructors in delivering the specific course proposed, or similar material if the course is new or customized for our events. Established curriculums that have been previously delivered will receive preference over similarly situated proposals for new courses.

Submission
Proposals should be submitted in writing to education@energysec.org. Proposals will be accepted on an ongoing basis, but preference for the 2019 events in Charlotte, NC and Austin, TX will be given to proposals received by Dec 31, 2018.

There is no prescribed format for proposals, but responses should address as much of the requested information as possible. Inquiries regarding this RFP may be directed to Steven Parker, steve@energysec.org.