



Energy Sector Security Consortium, Inc.

EnergySec and the DOE *Roadmap to Secure Control Systems in the Energy Sector*

Seth Bromberger
Director, EnergySec

I. Introduction and Scope

In 2006, the US Department of Energy, with the US Department of Homeland Security, published the *Roadmap to Secure Control Systems in the Energy Sector*, which “outlines a coherent plan for improving cyber security in the energy sector”. The *Roadmap* provides an overview of the current state of control systems security and proposes a comprehensive, multi-phased approach to establishing a strategic framework for improving the security within this critical sector.

In 2005, a group of security practitioners working for electric utilities in the Pacific Northwest founded the ESEC-NW information sharing organization. The organization grew quickly and, shortly after receipt of the National Cybersecurity Leadership award by SANS in 2008, renamed and expanded its scope to include asset owners across North America. Today, EnergySec has over 260 members representing over 90 organizations, over half the electricity distribution in the United States, and almost 40% of the generation. Information is exchanged in real time via a secure information sharing portal; an annual conference provides in-depth discussion of security topics relevant to the membership; and other programs designed to share best practices and insight into emerging security issues have been established.

Since its inception, EnergySec has been working to fulfill the vision of the *Roadmap* by directly addressing many of the milestone activities required for success.

II. The Roadmap

The *Roadmap*'s vision is ambitious and well-defined:

In 10 years, control systems for critical applications will be designed, installed, operated, and maintained to survive an intentional cyber assault with no loss of critical function.

The framework has four primary goals, one of which is directly served by EnergySec's mission:

Over the next 10 years, energy asset owners and operators are committed to working collaboratively with government and sector stakeholders to accelerate security advances.

Each goal has milestones that are categorized by implementation date into three tiers:

- Near term milestones - 0-2 years
- Mid term milestones - 2-5 years
- Long term milestones 5-10 years

In total, there are 23 milestones defined in the *Roadmap*.

III. *EnergySec's Roadmap Activities*

EnergySec has created its own matrix mapping current activities to the milestones described in the *Roadmap* [Table 1]. As new services are introduced, EnergySec will update this matrix.

For each of the milestones, the following indicators describe the role that EnergySec plays in the successful achievement of the task:

- **Perform / Partial Perform:** EnergySec currently performs this activity and can be counted on to maintain this activity on behalf of its membership. Activity directly relates to EnergySec mission and goals.
- **Assist:** EnergySec currently provides assistance to other organizations who are providing primary support for these activities. Activity indirectly relates to EnergySec mission and goals.
- **Capable:** EnergySec is capable of providing primary or assisting support for this activity when needed. Activity directly relates to and is compatible with EnergySec mission and goals. Development of capability dependent on funding or other external prerequisites.

In summary, of the 23 milestones defined in the *Roadmap*, EnergySec is currently performing two, actively assisting in four, and is capable of performing an additional four. Capability development is dependent on formalization of programs designed to achieve the milestone goals, which itself is dependent on financial support.

<i>Roadmap</i> Milestone	Supporting Goal	Term	EnergySec role / status
Consistent training materials on cyber and physical security for control systems widely available within the energy sector	Develop and Integrate Protective Measures	Near	CAPABLE. The EnergySec Information Sharing portal can be used both as a repository of training material and as a system of record for training completion.
Incident reporting guidelines published and available throughout the energy sector	Detect Intrusion and Implement Response Strategies	Near	CAPABLE. The EnergySec Information Sharing portal can be used both as a repository of response strategies and as a platform for collaboration on, and development of, additional strategies.

Roadmap Milestone	Supporting Goal	Term	EnergySec role / status
Major info protection and sharing issues resolved between the U.S. government and industry	Sustain Security Improvements	Near	PARTIAL PERFORM. EnergySec currently fulfills information sharing requirements among industry; government involvement has been limited but is growing. Issues still exist within government sector with respect to the processes surrounding information dissemination, especially when information is sourced from multiple agencies.
Industry-driven awareness campaign launched	Sustain Security Improvements	Near	CAPABLE. EnergySec currently provides awareness and training through conferences, presentations, and its annual summit. Formal awareness campaigns should be relatively straightforward to integrate into existing processes.
Common metrics available for benchmarking security posture	Measure and Assess Security Posture	Mid	ASSIST. EnergySec is providing collaboration, development, and dissemination tools for groups involved in this activity. EnergySec members would be primary stakeholders in this milestone.
Field-proven best practices for control system security available	Develop and Integrate Protective Measures	Mid	ASSIST. EnergySec is providing collaboration, development, and dissemination tools for groups involved in this activity. EnergySec members would be primary stakeholders in this milestone. EnergySec's Asset Owner members can identify current practice and field-test proposed practices.
Secure forum for sharing cyber threat and response information	Sustain Security Improvements	Mid	PERFORM. This is one of EnergySec's primary mission(s). Secure portal with multiple forums already exists.
Real-time security state monitoring for new and legacy systems commercially available	Measure and Assess Security Posture	Long	ASSIST. EnergySec is providing collaboration, development, and dissemination tools for groups involved in this activity. EnergySec members would be primary stakeholders in this milestone. A new situational awareness program, called SNAP, is currently being developed.

<i>Roadmap Milestone</i>	<i>Supporting Goal</i>	<i>Term</i>	<i>EnergySec role / status</i>
Control system network models for contingency and remedial action in response to intrusions and anomalies	Detect Intrusion and Implement Response Strategies	Long	ASSIST. EnergySec is providing collaboration, development, and dissemination tools for groups involved in this activity. EnergySec members would be primary stakeholders in this milestone.
Cyber security awareness, education, and outreach programs integrated into energy sector operations	Sustain Security Improvements	Long	CAPABLE. The EnergySec Information Sharing portal can be used both as a repository of training material and as a system of record for training completion. Additionally, EnergySec's Ask the Expert series, industry-developed whitepapers, and conferences provide additional information outlets and two-way forums for the exchange of information.

Table 1: EnergySec activity to Roadmap milestone mapping

IV. Summary

Because of its trust-based membership model and widespread industry acceptance, EnergySec is uniquely positioned to provide the effective information sharing and dissemination functions required to make the *Roadmap* vision a success. The EnergySec board of directors looks forward to discussing the most effective ways to partner with other organizations in order to help secure our nation's critical infrastructure.