# FINAL CHARTER - 07/16/2010

## UCAIug/OpenSG/SG Security Working Group
## Cyber Security Interoperability Task Force

## Background

The manner in which the energy sector is designing and operating control systems is undergoing some of the most significant changes in history due to the evolution of technology and the increasing number of interconnections to other system. With these changes come two significant challenges that the energy sector must face; 1) Cyber security is more important than ever before, and 2) Cyber security is more complicated than ever before. A key requirement in helping utilities and vendors alike in meeting these challenges is interoperability. While interoperability has been present in much of the discussions relating to technology utilized within the energy sector and especially the Smart Grid, it has been absent in the context of cyber security.

Collaboration between the SG Security Working Group within OpenSG and the Lemnos project will provide mutual benefits to each party. For Lemnos, the SG Security WG represents a long term steward for work products after project completion, a venue for industry review and feedback, as well as a "launch pad" for involving the Lemnos project with the Smart Grid mainstream. For the SG Security WG, Lemnos represents a tactical effort specifically focused on interoperability to support other efforts of the WG which are aimed at requirements.

## Goals

The goals of this Task Force shall include:

☐ Promote Interoperability of devices supporting cyber security functions

☐ Provide a forum and methodology to catalog and prioritize asset owner core security functional requirements

☐ Produce guidance for vendor and asset owners on configuration parameters for IP protocols utilized for cyber security

## Scope

The SG Security WG/Cyber Security Interoperability Task Force will coordinate its efforts with the Lemnos Interoperable Security Project, a multiyear DOE NSTB (National SCADA Test Bed) effort highlighting a security interoperability framework for communications supporting the energy sector. Partners in the Lemnos project include EnerNex, Tennessee Valley Authority, Sandia National Laboratories, and Schweitzer

# FINAL CHARTER - 07/16/2010

Engineering Laboratories. It is built on the successes of OPSAID (Open PCS Security Architecture for Interoperable Design), a previous NSTB project.

The Lemnos Project has developed a methodology for creating Interoperable Configuration Profiles. The methodology promotes matching of open source standards (IETF RFC's) to asset owner core security functional requirements. The Interoperable Configuration Profiles are created to be used within a control system environment and delineate the preferred options and details within the RFC's that are necessary for two devices to interoperate with one another.

The Task Force will assume long term responsibility for the methodology as well as Interoperable Configuration Profiles produced by the Lemnos project. At the completion of the current project (currently scheduled for Q1 2011), Lemnos is planned to produce the following Interoperable Configuration Profiles:

☐ IPSec

☐ Syslog standardization and use

☐ LDAP

☐ TLS/SSL and SSH

Further Task Force responsibilities shall include:

☐ The Task Force will maintain close coordination with Sandia National Laboratories in development of new or modification of existing Interoperable Configuration Profiles. Sandia will maintain a reference design implementation, contingent on funding, to facilitate testing by vendors wishing to adopt the use of the Interoperable Configuration profiles.

☐ Provide industry review and feedback forum for the methodology, catalog of core security functional requirements, and Interoperable Configuration Profiles

☐ Coordinate with other OpenSG efforts such as Conformance

## Leadership

Chair – Dave Teumim, Teumim Technical, LLC,
Vice-Chair - John Stewart, TVA
Secretary – Joe McCormick, Data Track Technologies

## Proposed Inter-relationship between the Lemnos Project and the Cyber Security Interoperability Task Force

# FINAL CHARTER - 07/16/2010

Near term (rest of 2010)

The SG Security WG/Cyber Security Interoperability Task Force provides review and feedback for new Interoperable Configuration Profiles being developed within the Lemnos Project.

As artifacts are finalized by the Lemnos team, they will be handed over to the Cyber Security Interoperability Task Force.

Long Term (2011 +)

The SG Security WG/Cyber Security Interoperability Task Force assumes ownership of Interoperable Configuration Profiles and reissues as OpenSG documents

The SG Security WG/Cyber Security Interoperability Task Force aids in transition of Lemnos effort from DOE NSTB effort to an industry/Smart Grid self-sustaining entity