National Electric Sector Cybersecurity Organization Resource (NESCOR) Final Technical Report

October 1, 2010 – June 30, 2014

DE-OE0000524

SEPTEMBER 2014

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS REPORT WAS PREPARED AS AN ACCOUNT OF WORK SPONSORED BY AN AGENCY OF THE UNITED STATES GOVERNMENT. NEITHER THE UNITED STATES GOVERNMENT NOR ANY AGENCY THEREOF, NOR ANY OF THEIR EMPLOYEES, MAKES ANY WARRANTY, EXPRESS OR IMPLIED, OR ASSUMES ANY LEGAL LIABILITY OR RESPONSIBILITY FOR THE ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION, APPARATUS, PRODUCT, OR PROCESS DISCLOSED, OR REPRESENTS THAT ITS USE WOULD NOT INFRINGE PRIVATELY OWNED RIGHTS. REFERENCE HEREIN TO ANY SPECIFIC COMMERCIAL PRODUCT, PROCESS, OR SERVICE BY TRADE NAME, TRADEMARK, MANUFACTURER, OR OTHERWISE DOES NOT NECESSARILY CONSTITUTE OR IMPLY ITS ENDORSEMENT, RECOMMENDATION, OR FAVORING BY THE UNITED STATES GOVERNMENT OR ANY AGENCY THEREOF. THE VIEWS AND OPINIONS OF AUTHORS EXPRESSED HEREIN DO NOT NECESSARILY STATE OR REFLECT THOSE OF THE UNITED STATES GOVERNMENT OR ANY AGENCY THEREOF.

THE FOLLOWING ORGANIZATION PREPARED THIS REPORT:

Electric Power Research Institute (EPRI)

Executive Summary

The goal of the National Electric Sector Cybersecurity Organization Resource (NESCOR) project was to address cyber security issues for the electric sector, particularly in the near and mid-term. The following table identifies the strategies from the DOE *Roadmap to Achieve Energy Delivery Systems Cybersecurity* published in September 2011 that are applicable to the NESCOR project.

Strategies	1. Build a Culture of Security	2. Assess and Monitor Risk	4. Manage Incidents	5. Sustain Security Improvements
Near-term Milestones **(0–3 years)** **By 2013**		2.1 Common terms and measures specific to each energy subsector available for baselining security posture in operational settings	4.1 Tools to identify cyber events across all levels of energy delivery system networks commercially available	
Mid-term Milestones (4–7 years) **By 2017**	1.4 Field-proven best practices for energy delivery systems security widely employed 1.5 Compelling business case developed for investment in energy delivery systems security	2.2 Majority of asset owners baselining their security posture using energy subsector specific metrics		5.3 Collaborative environments, mechanisms, and resources available for connecting security and operations researchers, vendors, and asset owners

Historically, cyber security research has concentrated on the Information Technology (IT) and Telecommunications sectors with an emphasis on information confidentiality. The NESCOR project focused on cyber security for control systems in the electric sector with an emphasis on system availability and integrity. Also, the electric sector has performance requirements that must not be degraded and contains legacy equipment with minimal or no cyber security controls. All of these differences in the electric sector require research to develop appropriate cyber security strategies, requirements, and technologies.

The NESCOR project had several sub-recipients but also relied on contributions from volunteers from utilities, academia, and the research and vendor communities. As the utilities were the primary recipient of the research results, it was important to have utilities participate on the various working groups.

The NESCOR project concentrated on:

- Assessing existing cyber security standards for domains of the electric sector, e.g., Distributed Energy Resources (DER) and Wide Area Monitoring, Protection, and Control

(WAMPAC), and cryptography standards;

- Developing guidance on penetration testing, vulnerability assessments, risk assessment, and design principles for the electric sector. This guidance built upon the guidance that was developed for the IT and telecommunications sectors;

- Developing failure scenarios that are intended to be useful to utilities for risk assessment, planning, procurement, training, tabletop exercises, and security testing. A cyber security failure scenario is a realistic event in which the failure to maintain confidentiality, integrity, and/or availability of sector cyber assets creates a negative impact on the generation, transmission, and/or delivery of power.

Finally, one of the goals was to ensure the sustainability of NESCOR. EPRI implemented several cost share projects that augmented and complemented the NESCOR projects. These projects will continue over the next several years. In addition, EPRI has established a NESCOR share point site that includes all of the deliverables produced throughout the term of the project. This share point site is available to current NESCOR participants.

TABLE OF CONTENTS

TABLE OF FIGURES

1. Background

Project Title: National Electric Sector Cybersecurity Organization Resource (NESCOR)

Award Period: October 1, 2010 – June 30, 2014

Recipient: Electric Power Research Institute, Inc. (EPRI)
Award Number: DE-OE0000524

Cost-Sharing Partner: Electric Power Research Institute, Inc. (EPRI)
Principal Investigator: Annabelle Lee

Project Team: The NESCOR project included the following sub-recipients: Adventium, ARC Technologies, EnerNex, InGuardians, Idaho National Laboratory (INL), N-Dimension, National Renewable Energy Laboratory (NREL), Oak Ridge National Laboratory (ORNL), Palo Alto Research Center (PARC), Sandia National Laboratory (SNL), Stanford Research Institute (SRI), Telcordia (renamed as TT Government Solutions), TLI (now Xpert Power Associates), University of California at Berkeley (UCB), University of California at Los Angeles (UCLA), University of Houston, UtiliSec, and Xanthus Consulting.

Project Objective: The objective of this project was to establish a National Electric Sector Cybersecurity Organization Resource (NESCOR) that had the knowledge and capacity to enhance the effort with the National Electric Sector Cybersecurity Organization (NESCO) by providing technical assessments of power system and cyber security standards to meet power system security requirements; provide recommendations for incident response, and participate in testing emerging security technologies in labs and pilot projects. NESCOR worked collaboratively to the extent possible with NESCO to focus research and development priorities and to identify and disseminate best practices; organize the collection, analysis and dissemination of infrastructure vulnerabilities and threats; and worked cooperatively with the Department of Energy and other federal agencies to identify areas where federal agencies with jurisdiction may best support efforts to enhance the bulk power electric grid and electric infrastructure.

This report includes the following:

- Overview of the technical working groups (TWGs)
- Summary and comparison of the actual accomplishments with the goals and objectives of the NESCOR project
- Project Activities Summary
- NESCOR projects and EPRI cost share projects descriptions
- Publications
- Presentations
- Sustainability of the NESCOR project

2. Overview of the Technical Working Groups (TWGs)

Included below is a high level summary of the planned focus areas for each of the four NESCOR working groups.

1. **Technical Working Group 1 (TWG1) – Threat and Vulnerability Assessment and Mitigation Group**
    a. TWG1 had two major responsibilities. The first was to collaborate and provide input to NESCO to address specific research areas that NESCO had identified as critical. The second was to identify specific research areas related to threats and vulnerabilities, define and develop research strategies, and produce actionable results.

2. **Technical Working Group 2 (TWG2) – Cybersecurity Requirements and Standards Assessment Group**
    a. Review NIST, NERC and other requirements and results and assess existing power system and standards to meet the security requirements of the power system

3. **Technical Working Group 3 (TWG3) – Cybersecurity Technologies Testing and Validation Group**
    a. Develop test plans for cybersecurity technologies to secure critical grid functions, facilitate security technology testing in EPRI substation lab, INL National SCADA Test Bed, UCLA SMERC Lab, etc.

4. **Technical Working Group 4 (TWG4) – Design Principle's Group (DPG)**
    a. Continue the work of the DPG that was performed under the National Institute of Standards and Technology Cyber Security Working Group (NIST CSWG).

3. Summary and comparison of the actual accomplishments with the goals and objectives of the NESCOR project

Listed below are the objectives for the NESCOR project and the accomplishments.

1. **Enhance the effort of with the National Electric Sector Cybersecurity Organization (NESCO) by providing technical assessments of power system and cybersecurity standards to meet power system security requirements;**

   Accomplishments:

   1. TWG1 team performed an assessment of the ZigBee Smart Energy Profile (SEP) 1.x specifications. Because the profiles were being deployed in several locations throughout the United States, the NESCOR team was tasked to provide recommendations on mitigating potential vulnerabilities. This effort was a combined effort by NESCOR and the National Institute of Standards and Technology (NIST) Cyber Security Working Group (CSWG).

   2. The primary focus of TWG2 was on standards analysis. The team published an assessment of the standards and requirements for Wide Area Monitoring, Protection, and Control (WAMPAC) and Distributed Energy Resources (DER). The WAMPAC report summarizes findings related to the cyber security requirements as reflected in the WAMPAC standards. The scope of the DER report was to describe the cyber security requirements for DER, reflecting DER functions in the smart grid and taking into account variations of DER architectures.

   3. TWG4 performed an assessment of the IEC 62351 family of standards, focusing on cryptography and role based access control (RBAC). Comments were submitted to IEC TC57/WG15.

   4. EPRI finalized and submitted the draft Lemnos IPSEC protocol interoperable configuration profile (ICP), designated the IEEE 2030.102.1 standard, with updated requirements, to the IEEE Power and Energy Society (PES) Substation working group C16. The standard is now out for review.

   5. EPRI reviewed the IEC 62351-7 standard and defined network security management objects that can be implemented in end systems. Feedback was provided on the standard to IEC TC57/WG15.

   6. NESCOR, in conjunction with NESCO, submitted comments on the NERC CIP V5 standards drafts, focusing on the technical content of the various draft standards.

   7. EPRI produced a report that identified some emerging solutions to protect the privacy of energy usage data while allowing utilities and third parties to perform functions on the aggregated data.

2. **Provide recommendations for incident response**

Accomplishments:

8. The first step in managing cyber security incidents involves detecting when they occur. An Integrated Security Operations Center (ISOC) brings together the many isolated monitoring and response functions in a unified framework. In 2013, EPRI developed guidance for planning an ISOC. (The work continues in 2014. See description below.)

9. With the widespread deployment of large-scale Advanced Metering Infrastructure (AMI) systems, utilities must address the task of managing the alarms and events that are generated by the meters. EPRI developed a report documenting standard security objects for AMI systems.

3. **Participate in testing emerging security technologies in labs and pilot projects.**

Accomplishments:

10. EPRI has established a Cyber Security Research Lab (CSRL) in the Knoxville, TN facility[1]. TWG3 performed in-lab security testing and validation in the WAMPAC Smart Grid domain with the primary goal of validating the testing tasks contained in the TWG3 NESCOR Guide to Penetration Testing. This testing will continue in 2014. In addition, EPRI conducted a “plug-fest” for the DNP3 SA V5 standard in Sept 2014. (See description below.)

4. **Work collaboratively to the extent possible with NESCO to focus cyber security research and development priorities and to identify and disseminate best practices;**

Accomplishments:

11. The primary activity of TWG1 was to develop a family of cyber security failure scenario and impact analyses documents. The failure scenarios address cyber security compromises that are a result of malicious and non-malicious activity. The goal was to identify specific failures, specify applicable vulnerabilities, and define mitigation strategies. The scenarios are not at a detailed level that would allow an attacker to compromise components of the existing grid nor do they define specific technologies.

12. TWG3 developed the guide to penetration testing and the guide to vulnerability assessment and focused on the electric sector and control systems. Previous penetration testing and vulnerability assessment guidance focused on IT and telecommunications systems.

13. EPRI produced a report that identified the design principles applicable to AMI and the management of cryptographic keys.

14. EPRI developed guidance on risk assessment in coordination with DOE, using the methodology included in the NESCOR failure scenarios and impact analyses document. (This work is continuing in 2014 with additional

[1] 1 EPRI members provided funding for the CSRL, and not part of the NESCOR cost share project.

collaboration in security metrics.)

15. EPRI complemented the NESCOR “Cybersecurity Requirements for Distributed Energy Resources (DER) Systems” document by proposing a set of actionable security measures for utilities.

16. EPRI developed a report that establishes a framework for selecting measurements to score the performance of cyber security functions built into a supplier’s products and services.

5. Organize the collection, analysis, and dissemination of infrastructure vulnerabilities and threats;

Accomplishments:

17. EPRI developed a report on combined cyber-physical attack scenarios for the electric sector. The scenarios described in the report encompass the three infrastructure domains of generation, transmission, and distribution.

18. The failure scenarios and impact analyses documents identify common vulnerabilities and threat agents.

6. Work cooperatively with the Department of Energy and other Federal agencies to identify areas where Federal agencies with jurisdiction may best support efforts to enhance cyber security of the bulk power electric grid and electric infrastructure.

Accomplishments:

19. The NESCOR teams and EPRI coordinated with NIST, DOE, and DHS in the development and revision of the various NESCOR documents, particularly the failure scenarios and impact analyses family of documents.

20. NESCOR participated in briefings with several federal agencies, such as the FBI, DOD, and intelligence agencies on the NESCOR projects.

4. Project Activities Summary

Following is a summary of the various NESCOR projects and EPRI cost share projects, including the original hypotheses, approaches used, problems encountered, departure from planned methodology, and an assessment of the impact from problems. The summary is organized by working group.

Overall Assessment: Overall, the NESCOR project has been very successful. Utilities, vendors, and the research community use the failure scenarios and impact analyses documents worldwide. The penetration-testing document is the first to address the topic for control systems. The WAMPAC report focuses on an area with few experts. Many of the original NESCOR volunteers are interested in continuing on some of the efforts – such as the failure scenarios. In addition, the EPRI cost share projects have leveraged several of the NESCOR projects. These cost share projects are continuing this year and will continue in future years.

TWG1: The SEP 1.x project was a short-term task intended to provide technical guidance on potential vulnerabilities and mitigations in the SEP 1.x protocols. Leading cryptography experts from around the world participated in providing the assessment. The resulting document has been distributed and used worldwide.

The primary focus of TWG1 was the development of the family of failure scenarios and impact analyses documents. Previously, federal agencies have developed attack scenarios for many of the critical infrastructures, but typically the content is classified. The goal was to develop scenarios that would be publicly available for the electric sector. The team spent the entire award period developing and revising the various documents. In addition, there were many volunteers from utilities, academia, and vendors that participated in the development and review of the documents. The goal was expanded to include the development of common mitigations, common vulnerabilities, and a risk assessment methodology. This work is the basis for several EPRI projects, as documented below. In addition, the failure scenarios document has been used by several DOE labs and by the University of Illinois in research projects. Finally, the document has been distributed worldwide to research organizations and utilities.

The EPRI Integrated Security Operations Center (ISOC) project was initiated in response to requests from utilities trying to coordinate security events. This is an emerging critical area. The first task was to document how to plan an ISOC. This work continues and is being expanded.

TWG2: The initial focus areas for the team were in WAMPAC, DER, and privacy. The technical leads for the WAMPAC and DER projects are considered experts. The WAMPAC report has been used by several standards working groups. The DER report included architecture diagrams that have been included in several other documents. As a future DER task, criteria could be included to assist users in selecting the various cyber security requirements. To ensure there was no duplication of tasks, the NESCOR privacy team members participated in the NIST Cyber Security Working Group (CSWG) Privacy team. The objective was to augment the work of the CSWG and to keep the TWG2 informed of the CSWG work. The EPRI Network Security Management (NSM) project was tasked to propose revisions to the IEC 62351-7 standard. The objects in the existing standard are difficult to implement. The EPRI team coordinated with the IEC working committee and several utilities to address this issue – and the report has been used by IEC to update the standard.

TWG3: The focus was to develop test guides for performing security assessments and penetration testing and perform security testing of proposed security solutions. The approach was to provide guidance on assessing control system devices. The current guidance focuses on IT and telecommunications devices. TWG3 identified a series of documents that would provide this guidance. Two documents were completed: Guide to Penetration Testing and Guide to Vulnerability Assessment. The penetration-testing guide was the major focus and has been extensively used and included in several training courses. There is also an open source framework of tools available that is based on the penetration-testing guide. The vulnerability assessment guide was recently posted. The other documents identified by TWG3 are: *NESCOR Guide to Security Posture Assessment,* the *NESCOR Guide to Network Capture Analysis, and the NESCOR Guide to Physical Security Assessments.* These could be developed in the future.

With the establishment of the EPRI Cyber Security Research Lab (CSRL)[2], testing of various security products, security protocols, and security architectures included in the various NESCOR and EPRI cost share deliverables will be performed. This is important for the continuation of the NESCOR activities beyond the completion of the award.

TWG4: The team continued the work that had been started by the NIST Design Principles Group (DPG). The team reviewed and commented on several of the IEC 62351 standards, and focused on the cryptography sections. These comments were sent to IEC. Work continued on the design principles for the Advanced Metering Infrastructure (AMI) and the document was finalized and published by EPRI.

NESCO Coordination: DOE funded both EPRI (NESCOR) and EnergySec (NESCO) for the projects. As part of the award, it was important for NESCOR and NESCO to coordinate their work. Because there was no duplication of effort between the two projects, communication was not as critical as initially envisioned. One of the NESCOR projects (TFE assessment) was performed at the request of NESCO. Also, NESCO and NESCOR collaborated in submitting comments to NERC on the draft NERC CIP V5 standards. Finally, NESCO presented and participated in the annual NESCOR workshops.

Program Management Coordination: The second PI for NESCOR took over the role late in 2011. Initially, there were 17 sub-recipients on the project, including several DOE labs. Having so many sub-recipients is a significant management task. The new PI reorganized the sub-recipients to better align their skills with the tasks of the working groups. This resulted in a more strategic organization that required less subject matter experts to lead the various efforts. Also, the PI worked with the utility volunteers to ensure that their key issues and concerns were being addressed and that the various products met their needs. Finally, each TWG was co-lead by EPRI and one or more of the sub-recipients. Each team had a regularly scheduled call to discuss the various work products and the status. The EPRI team leads had regular discussions to ensure that there was no duplication in work effort, that the various products complemented each other, and that the major research issues were addressed. Every deliverable document was technically reviewed by the EPRI management team to ensure that the technical content was accurate and that the product was useful to utilities.

[2] EPRI members provided funding for the CSRL, and not part of the NESCOR cost share project.

5. NESCOR Projects and EPRI Cost Share Projects Descriptions

Included below are descriptions of the various NESCOR projects that were performed by the TWGs and the cost share projects performed by EPRI. The cost share projects are listed with the applicable TWG.

5.1 TWG1 - Threat and Vulnerability Assessment and Mitigation Group Update

5.1.1 NESCOR Projects

Technical Feasibility Exception (TFE): The NESCO/NESCOR Common TFE Analysis project aimed to investigate commonly filed Technical Feasibility Exceptions (TFEs) to the NERC CIP requirements. The expectation of the project team is that TFEs filed for the same issue by many utilities indicate either a difficult security problem requiring a solution, or a problem with the CIP requirements, or both. A combined NESCO/NESCOR team assessed TFE Category NERC CIP-007-4 R5.3 that specifies password complexity requirements for critical cyber assets. Many utilities are filing TFEs to this requirement for Microsoft Windows systems because these systems cannot enforce the requirements. The results were documented in the NESCOR report, *NESCO/NESCOR Common TFE Analysis: CIP-007 R5.3 Password Complexity*, published in 2011.

SEP 1.x: TWG1 performed an assessment of the ZigBee Smart Energy Profile (SEP) 1.x specifications. The Smart Grid Interoperability Panel (SGIP) CSWG had reviewed both the SEP 1.0 and 1.1 profiles and identified potential security vulnerabilities. Because the profiles were being deployed in several locations throughout the United States, the NESCOR team was tasked to provide recommendations on mitigating potential vulnerabilities. This effort was a combined effort by NESCOR and the NIST Cyber Security Working Group (CSWG). In addition, several individuals with relevant expertise participated in the analysis. The document includes a discussion of potential implementation issues that need to be addressed. These implementation issues are outside the scope of the SEP 1.x specification, but important to ensure the security of any implementation. Also included is information on the California and Texas deployments of Home Area Networks (HANs) and SEP 1.x requirements. The results are documented in the NESCOR report, *Smart Energy Profile (SEP) 1.x Summary and Analysis*, published in October 2011.

Failure Scenarios and Impact Analyses: TWG1 developed several documents on the topic of cyber security failure scenarios and impact analyses for the electric sector. The information about potential cyber security failure scenarios is intended to be useful to utilities for risk assessment, planning, procurement, training, tabletop exercises, and security testing. A cyber security failure scenario is a realistic event in which the failure to maintain confidentiality, integrity, and/or availability of sector cyber assets creates a negative impact on the generation, transmission, and/or delivery of power.

The failure scenarios were developed from a “bottom-up,” rather than a top-down assessment of potential cyber security events. Their focus is on cyber security events; hence, they do not consider requirements that are outside this scope (e.g., redundancy that supports reliability, general cyber-physical requirements such as range checking for values, etc.). The vulnerabilities and mitigations for all scenarios use a common naming schema that improves readability and comprehension, and enables their prioritization. Mitigations are intended as suggested recommendations that provide a variety of options. The development of the common mitigations and common vulnerability classes was based on comments received from Inmetro and various utilities. The former lead of the NIST CSWG vulnerability working group participated in the development of the common vulnerability classes for the failure scenarios.

The failure scenarios are not intended to be a complete list of all possible failure scenarios. Rather, they are a useful representative list of the cyber security challenges facing the electric sector. To support the failure scenario and impact analyses documents, TWG1 developed an excel toolkit. Following is a list of the NESCOR failure scenario documents and the toolkit:

- *NESCOR Failure Scenarios and Impact Analyses, V2.0*, June 2014
- *NESCOR Failure Scenarios Toolkit*, June 2014
- *NESCOR Common Vulnerabilities and Mitigations Mapping, September 2013*
- *Analysis of Selected Electric Sector High Risk Failure Scenarios*, September 2013
- *Attack Trees for Selected Electric Sector High Risk Failure Scenarios*, September 2013

Related Activity: The organization Inmetro in Brazil has leveraged TWG1's failure scenario concepts to create failure scenarios of their own that are specific to smart meters. TWG1 members and EPRI NESCOR had several telecons on the scenarios developed by Inmetro. TWG1 developed detailed written comments and held a technical teleconference with Inmetro to discuss these comments. Highlights of these comments were the suggestion to create a smart meter external interface "model" on which to base the scenarios, the addition of integrity controls to the mitigation list, and the importance of examining attacks that would impact multiple meters.

5.1.2 EPRI Cost Share Projects

Procurement Requirements: This technical update established a framework for selecting measurements to score the performance of cyber security functions built into a supplier's products and services. It leverages EPRI's procurement methodology published in other EPRI technical update reports and the *Guidelines for Smart Grid Cyber Security* specified in National Institute of Standards and Technology Interagency Report (NISTIR) 7628. The procurement framework is necessary to guide the development of procurement language and a grading scheme for a utility to select more advanced cyber security solutions that are tailored for power delivery systems. The research reported in this technical update establishes a workflow to select cyber security evaluation criteria using the requirements specified in NISTIR 7628. A substation automation system (SAS) is used as an example of applying the criteria to selected NISTIR 7628 access control requirements. The results are documented in *Framework for Grading Procurement Requirements for Power Delivery Systems*, EPRI Technical Update 3002001041 published in December 2013.

Integrated Security Operations Center: The first step in managing cyber security incidents involves detecting when they occur. However, the complexity of power systems often makes it difficult to detect when attacks are under way. Although individual intelligent electronic devices (IEDs) and systems may produce alerts and alarms for security events, they are often not correlated across distributed systems. Traditional intrusion detection systems (IDS) and security information and event management (SIEM) systems need to be tailored to understand attack profiles for power systems. This includes correlating the geographical and temporal nature of events. Additionally, events need to be correlated with the power system data to provide a complete situational awareness.

Security Operations Centers (SOCs) are common in physical security, business, and industrial control environments. Many organizations have one or more of these individual SOCs responsible for defined physical regions or business functions. As the threat landscape has evolved, there is a greater need to have a coordinated view of security events across an organization’s entire enterprise. An Integrated Security Operations Center (ISOC) brings together the many isolated monitoring and response functions in a unified framework. This project focused on guidelines for designing an ISOC.

The project had the following objectives:

1. Create an event correlation test bed for testing IDS and SIEM solutions in EPRI’s Cyber Security Research Lab
2. Develop guidelines to build an ISOC
3. Develop methodologies to perform event correlation across distributed power systems and conduct initial tests in EPRI’s laboratories

This project began in Q1 2013 and continues in 2014. The deliverable for 2013 was *Guidelines for Planning an Integrated Security Operations Center,* EPRI Technical Update 3002000374***.*** This report describes strategies and best practices for utilities to plan and implement an ISOC that includes corporate systems, control systems, and physical security. The research focused on the initial steps in the process of setting up an ISOC: developing the business case, potential organizational challenges, creating requirements for log collection, management, and analysis, translating these requirements into an ISOC architecture, and incorporating threat assessment capabilities**.** These results were based on current research, engagement with utilities, and an examination of ISOC implementations outside of the electric sector.

Future Activities: In 2014, EPRI has focused on three key activities to support the incident management and ISOC research. First, EPRI has led the ISOC Task Force that is a group of member utilities that are in various stages of their own ISOC implementation. This group is helping to drive the research and establish best practices for ISOC implementation. Second, EPRI is implementing various SIEM solutions in its Cyber Security Research Lab. This provides (1) a testing environment for members to test and try out various SIEM solutions, and (2) the test bed for EPRI to conduct testing for ISOC threat scenarios. Third, the research is focusing on developing guidelines for the process of integrating the physical and cyber security monitoring of control center systems into an ISOC: understanding potential security failure scenarios, developing the requirements, analyzing the impact of NERC CIP regulation on the requirements, understanding the impact of different ISOC architectures on the security monitoring process, and guidelines for the implementation process. These results are based on current research, engagement with utilities, and an examination of ISOC implementations outside of the electric sector.

Risk Assessment and Mitigation Strategies: This project builds upon the TWG1 failure scenarios and impact analyses products. There are several EPRI cost share projects and each is described below.

<u>Draft Risk Assessment</u>: This project built upon the work that was completed in 2011 in the development of attack/failure scenarios and developed scenarios that focused on coordinated cyber-physical attacks. These scenarios include the threats and vulnerabilities that may be exploited by a well-financed and motivated nation-state. A mechanism for breaking down the scenarios into small functional components, referred to as decomposition, is applied to each scenario. An analysis of the resulting decomposition is then used to identify guidelines asset owners and operators can use in determining the impact of each attack/failure. The results are documented in EPRI Technical Update, *Draft Risk Assessment Processes*, 1024422 published in December 2012.

<u>Risk Mitigation Strategies</u>: This project built on the development of attack/failure and cyber-physical attack scenarios focused on combined cyber-physical attacks. These scenarios include threats and vulnerabilities that may be exploited by well-financed and motivated entities. This report also leverages risk assessment processes developed to address combined cyber-physical attack scenarios. The framework in this update supports the further development of risk mitigation strategies focused on combined cyber-physical attacks. EPRI, *Risk Mitigation Strategies*, Technical Update1024423, December 2012.

<u>Integrating Failure Scenarios</u>: In 2013, EPRI published Technical Update *Integrating Electricity Subsector Failure Scenarios into a Risk Assessment Methodology,* 3002001181. This technical update provides guidance to utilities on developing and implementing a risk assessment process using the failure scenarios developed by the NESCOR project. This document was jointly published by EPRI and DOE and is available on both websites.

Future Activities: For 2014, EPRI will continue the collaboration with DOE and further expand the risk assessment document and develop a risk assessment framework that coordinates and maps several documents, such as the DOE ES-C2M2, the NISTIR 7628, the NESCOR failure scenarios and risk assessment approach, and the NIST Cybersecurity Framework. The goal is to provide guidance on how all these requirements/guidance documents are associated and how they may be used to determine cyber security risk. American Public Power Association (APPA), National Rural Electric Cooperative Association (NRECA), Edison Electric Institute (EEI), and several utilities have joined the work effort.

LEMNOS: LEMNOS interoperable configuration profiles (ICPs) can be used to ensure interoperability for a given network protocol within a mixed vendor environment. The ICPs for IPSec and SSH ICPs were completed and tested by six vendors during an interoperability test in August 2011.

The draft LEMNOS IPSec protocol ICP, designated the IEEE 2030.102.1 standard, has been submitted with updated requirements and is out for review by IEEE Power and Energy Society (PES) Substation working group C16. In addition, the upgraded draft standard is being tested between two different vendors' devices. The IPSec configuration and test results were documented in an EPRI technical report that was released in 2013, *Lemnos Implementation Guide for IPSec, Device Configuration Examples,* EPRI Technical Update 3002000375. In January through May of 2014, the working group and vendors discussed outstanding issues of the proposed standard. In the May 2014 WG meeting, a restructuring of the document was agreed upon and created a “Profile A” and a “Profile B” for the standard. “Profile B” addresses the option to use network address translation traversal (NAT-T).

Future Activities: IEEE 2030.102.1 Draft 5 (D5) of the standard is currently under review and will be submitted for balloting. If necessary, a comment resolution process will occur before approval and publishing of the standard. The next in-person meeting occurred in Sept 2014, where the revised scope and purpose need to be approved to align with the latest draft of the standard.

Table Top Exercises: With the deployment of more automated equipment and the increasing interconnection of systems and devices in the electric sector (including IT and telecommunications equipment), tabletop exercises that assess preparedness for cyber security events have become increasingly important.

Future Activities: In 2014, EPRI will be developing procedures for running cyber security table top exercises and assessing the results, developing cyber security tabletop exercise scenarios for the electric sector, conducting tabletop exercises at the member sites, and presenting the results at a webinar. The cyber security scenarios will be based on the failure scenarios documented in the NESCOR report.

5.1.3 Additional EPRI Tasks

Failure-Driven Specification-Based Intrusion Detection System (IDS): This project is building upon the initial work performed by NESCOR and the University of Illinois Trusted Cyber Infrastructure for the Power Grid (TCIPG). TCIPG has developed a specification-based IDS for AMI. This system is designed to monitor the traffic among meters and access points at the network, transport, and application layers. The specification-based detection technology ensures that AMI devices are running in a secure state and that their operations respect a specified security policy. The testing operations are guided by the threats identified in the cyber security failure scenarios developed by the NESCOR team. (The final report is pending.)

Risk Metrics: The monitoring of the controls in place and the output of useful metrics can be used to benefit and improve a utility's cyber security program. Such metrics could also be used to provide senior management with an ongoing reporting process and support cyber security investment decisions in areas such as hardware, software, and personnel resources. The evaluation framework that was developed in 2013 used both the ES-C2M2 and the NISTIR 7628 in determining the security posture of systems.

Future Activities: For 2014, EPRI will produce a technical update that builds upon the previous evaluation framework, provides guidance for all 10 domains in the ES-C2M2, and allocates NISTIR 7628 security requirements to specific practices within the 10 domains. The current ES-C2M2 document focuses on organization-level maturity. Therefore, recommendations will be made on how to tailor the ES-C2M2 for determining the security posture of utility systems.

This document will be developed jointly by EPRI, DOE, APPA, EEI, NRECA, and several utilities and will be coordinated with the *Risk Assessment Framework* document that will be produced by EPRI and DOE in 2014.

5.2 TWG2 - Cybersecurity Requirements and Standards Assessment Group

5.2.1 NESCOR Projects

NERC CIP V5 draft documents: NESCOR, in collaboration with NESCO, provided comments on two draft versions of the NERC CIP V5 draft standards. The focus was to identify the major technical issues with the proposed standards. 14 individuals participated in reviewing the standards and submitting comments. The comments were sent to NERC in January and May 2012 and are posted on the EPRI NESCOR site.

Advanced Metering Infrastructure (AMI) Remote Connect/Disconnect (RC/D): The AMI RC/D project team task was moved to the NIST CSWG. The AMI experts on TWG2 coordinated tasks between the two groups.

Data Privacy: To ensure there was no duplication of tasks, the NESCOR privacy team members participated in the NIST CSWG Privacy team. The objective was to augment the work of the CSWG and keep the TWG2 informed of the CSWG work.

Wide Area Monitoring, Protection, and Control (WAMPAC) requirements: The WAMPAC concept was described in a document developed by an informal industry group that was advising the Transmission and Distribution (T&D) Domain Expert Working Group (DEWG) in NIST. Such systems constitute a suite of different system architectures aimed at meeting various application requirements.

The WAMPAC report summarizes findings related to the cyber security requirements as reflected in the WAMPAC standards. The findings are discussed in the context of the published WAMPAC Advanced Security Acceleration Project for the Smart Grid (ASAP-SG) and the NISTIR 7628 reports, on-going WAMPAC related standards development, existing cyber security standards, and on-going cyber security reviews of standards conducted through the Smart Grid Interoperability Panel (SGIP).

The report presents a few WAMPAC implementation scenarios, where the standards are used for end-to-end applications. In such scenarios, the gaps regarding cyber security aspects of the entire solution are addressed. Suggestions for how to bridge the gaps in future designs are outlined at the end. The NESCOR report is *Wide Area Monitoring, Protection, and Control (WAMPAC): Standards for Cyber Security Requirements* and was published October 2012.

Distributed Energy Resources (DER) Systems: The scope of the NESCOR report was to describe the cyber security requirements for DER, reflecting DER functions in the smart grid and taking into account variations of DER architectures. These DER architectures are mapped to the DER Actors, Logical Interfaces, and Logical Interface Categories (LICs) in the NISTIR 7628, including proposed updates to the existing actors and logical interfaces. The NISTIR 7628 high-level security requirements that are associated with the LICs are assessed for applicability to these DER architectures. In addition, DER-specific issues are discussed. The NESCOR report is *Cyber Security for DER Systems, Version 1.0* and was published in July 2013.

5.2.2 EPRI Cost Share Projects

Security Architectures for Integrating Distributed Energy Resources into the Grid: The goal of this project was to complement the NESCOR “Cybersecurity Requirements for Distributed Energy Resources (DER) Systems” document by proposing a set of actionable security measures for utilities. These security measures were developed based on generic use cases for various types of connections to the electrical grid: dedicated medium-voltage (MV) feeder, shared MV feeder, or low-voltage (LV) feeder. The primary focus was how to integrate DER into the grid so that cyber security risks to the power delivery system are mitigated. There are two ways to use this report. First, if a utility plans to deploy DER and would like to understand best practices, it can refer to the report’s recommendations. Second, if a utility has already deployed DER, it may want to check its controls against best practices.

The deliverable for this project was *Security Architectures For Integrating Distributed Energy Resources Into the Grid,* EPRI Technical Update 1024425 published in 2012.

Standardized Security Objects for AMI: With the widespread deployment of large-scale Advanced Metering Infrastructure (AMI) systems, utilities must address the task of managing the alarms and events that are generated by the meters. However, AMI systems do not easily integrate into SIEM systems and IDSs due to the fact that AMI vendors do not use standard data objects for representing the alarms and events that are generated by the meters. This project addresses this issue by developing standard security objects for AMI systems. Creating a common definition for the structure, content, and semantics of AMI alarms and events will increase the security interoperability for AMI systems, ensure that a common set of security objects is supported, and enhance the integration of AMI systems with SIEMs and IDSs. The deliverable for this project was *Advanced Metering Infrastructure Security Objects,* EPRI Technical Update 1024427 and was published in 2012.

Assessment of Privacy Technology to Support Protection of Energy Usage Data: The goal of this project was to build upon the work performed by NESCOR TWG2/NIST CSWG and examine current and proposed technology to address privacy issues associated with consumer energy usage data. With over 20 million smart meters deployed in the US and multiples of that number deployed worldwide, technologies to protect consumers’ privacy are still maturing. The report identifies some emerging solutions to protect the privacy of energy usage data while allowing utilities and third parties to perform functions on the aggregated data. The results of the project are documented in *Assessment of Technology Used to Protect the Privacy of Energy Usage Data*, EPRI Technical Update 1024426, published in 2012.

Transmission Systems Network Security Management: The objective of the project was to identify where network and system management (NSM) standards/technology are applicable to the bulk electric transmission system for enhanced situational awareness, security, reliability and system confidence as network intelligence advances. This research effort engaged with the International Electrotechnical Commission (IEC) Technical Committee (TC) 57 Working Group (WG) 15 to promote the standardization and interoperability of these objects. This project provided a set of NSM use cases, resulting requirements, and a review of the IEC 62351-7 standard. A demonstration trial was implemented to show the end-to-end functionality of a Network and System Manager. (Note: the next project builds on this work.) The deliverable for the project was *Network Security Management for Transmission Systems*, EPRI Technical Update 1024421 and was published in December 2012.

Network Security Management (NSM): The objective of this project was to identify where NSM standards/technology are applicable and valuable to the bulk electric transmission system for enhanced wide area situational awareness, security, reliability and system confidence as network intelligence advances. The project provided several “Use Cases” that are intended to identify the actors and objectives of a system’s solution set and to generate utility and vendor input on the challenges being tackled, solutions being addressed, and effectiveness of the standardized solution work proposed. Given the increasing level of automation and Information and Communication Technologies (ICT) being deployed within the bulk electrical system, it is also necessary to discuss at a high level how new intelligence creates unforeseen challenges to grid operations that would be addressed by an NSM standard. Additionally, the International Electrotechnical Commission (IEC) 62351-7 standard for common information security objects was reviewed with feedback provided to the IEC Technical Committee (TC) 57 Working Group (WG) 15.

The EPRI Technical Update *Network System Management: End System Related IEC 62351-7 Object Definitions*, 3002000373 was published in 2013. This report concretely defined IEC 62351-7 Network Security Management (NSM) objects in a manner that can be implemented and supported by intelligent electronic devices (IEDs), SNMP Gateways, and other end systems.

Future activities: In 2014, EPRI will demonstrate a number of scenarios and use cases. Some examples are:

1. Network discovery
2. Substation Network Status and Traffic Analysis
3. Alarm when traffic exceeds pre-defined threshold
4. Turn off a switch port with “rogue” device
5. Use cases to be tested with the SNMP Gateway
    - Protocol Error and Critical Event
    - Idle Time and Denial of Service
    - Login Failure Detection

The research results, along with a demonstration of the various scenarios and uses cases will be presented at EPRI’s Utility Workshop on October 29, 2014.

5.3 TWG3 - Cybersecurity Technologies Testing and Validation Group

5.3.1 NESCOR Projects

NESCOR Guide to Penetration Testing for Electric Utilities: The report was created for electric utilities to use in their security assessment of smart grid systems. Smart grid security assessments can be broken into several categories. The document focuses only on penetration testing and attempts to help utilities break down the complex process of penetration testing. Penetration testing is a specialized form of hands-on assessment where the testing team takes on the role of the attacker and tries to find and exploit vulnerabilities in systems and devices.

The report breaks the process of penetration testing into logical tasks. These tasks are organized into logical categories based on the skill set of the testing team, each category represented by major sections in this document. Because of the nature of penetration testing, the tasks in the document are high level and intended to break the overall penetration test into logical components that can be assigned to testing team members to be completed in a systematic manner. The report is *NESCOR Guide to Penetration Testing for Electric Utilities, Version 3,* and was published in July 2013.

Related Work – Penetration Testing Framework: To facilitate the use of the NESCOR Guides for electric utilities, UtiliSec has created an open source framework of tools based on the NESCOR Guide to Penetration Testing. This framework is named the "Samurai Security Testing Framework for Utilities" and is freely available for download by electric utilities worldwide at www.SamuraiSTFU.org.

NESCOR Guide to Vulnerability Assessments for Electric Utility Operations Systems: This report provides guidance on vulnerability assessments for electric utilities. The objective of a vulnerability assessment as described here is to develop an in-depth view of a utility's security posture with a focus on system and network vulnerabilities. Results from a vulnerability assessment can be used to determine or recommend mitigations for the utility. A vulnerability assessment can serve as a key component in assessing a utility's overall cyber security posture and the results can be used to assist in prioritizing a utility's operating plans, programs, and budgets. The report is *NESCOR Guide to Vulnerability Assessment for Electric Utility Operations Systems, Version 1.0* and was published in June 2014.

Future Activities: NESCOR Guide to Validation and In-Lab Security Testing: TWG3 performed in-lab security testing and validation in the WAMPAC Smart Grid domain with the primary goal of validating the testing tasks contained in the TWG3 NESCOR Guide to Penetration Testing. This work is continuing and is being performed in EPRI's WAMPAC lab facilities in Knoxville, TN. This effort is performed in collaboration with the EPRI cost-share project "Penetration Test Procedures for Wide-Area Monitoring, Protection and Control". The deliverable from this effort will be published in 2014 and will be in a document describing the procedural level steps of the penetration testing tasks when used on sample WAMPAC systems.

5.3.2 EPRI Cost Share Projects

DNP3 Secure Authentication version 5: The EPRI DNP3 secure authentication v5 project has two objectives:

- The first is to increase utility education and awareness of implementation strategies and potential related issues. To accomplish this, EPRI gave a presentation at a high-level education session. EPRI will also have a 2 day detailed utility workshop focused on the implementation details.

- The second is to increase vendor adoption of DNP3 SAv5. To accomplish this, EPRI will bring IED vendors into the lab to test their DNP3 SAv5 implementations with test scenarios developed in conjunction with utilities and vendors.

Future Activities: In 2014, EPRI will:

- Conduct a high level education session
- EPRI hosted an interoperability testing workshop in the EPR Cyber Security Research Lab September 15-17, 2014. Twelve vendors that have implemented DNP3 SAv5 into their products attended this event.
- EPRI is hosting a utility workshop on November 6, 2014 to provide demonstrations of use cases among the various vendors that have adopted the DNP3 SAv5 standard. In addition, an overview of the “DNP3 SAv5” migration guide will be presented. This guide is one of the 2014 project deliverables.

The following diagram illustrates the draft DNP3 SAv5 demonstration environment and the vendors that were part of the interoperability test.

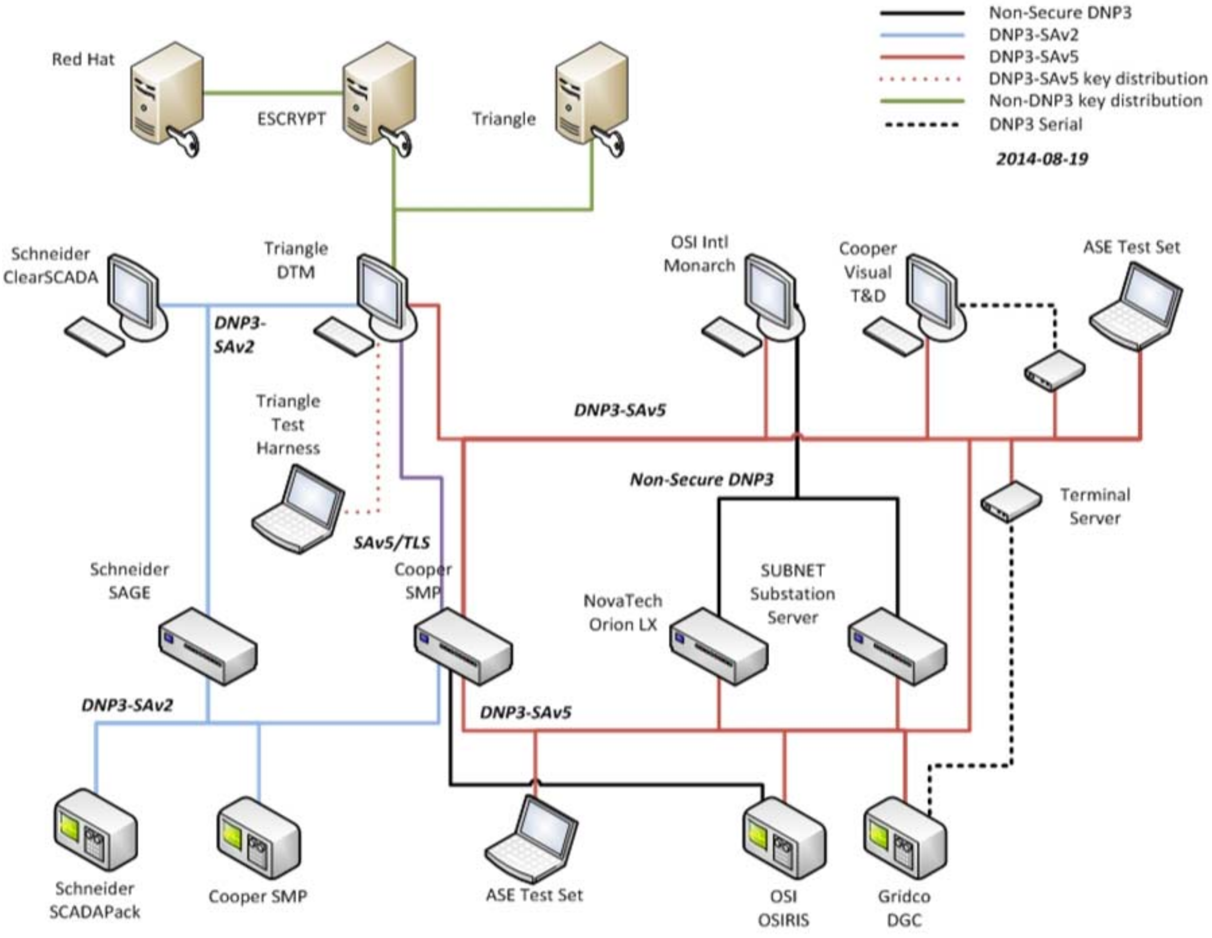

Figure 1: DNP3 SAv5 Demonstration Environment

5.4 TWG4 – Design Principles Group

5.4.1 NESCOR Projects

EPRI has negotiated an agreement with ANSI to provide access to the approved standards in the IEC 62351 family - including parts 1 through 8. TWG4 built on the work of the CSWG and performing an assessment across the various standards to ensure consistency, interoperability, and up-to-date protocols and cryptography primitives. The recommendations were submitted to IEC TC57/WG15, specifically in parts 2 (Glossary of Terms), 3 (Communication Network and System Security – Profiles Including TCP/IP), and 8 (role-based access control).

5.4.2 EPRI Cost Share Projects

Cryptographic Key Management (CKM) Design Principles for the Advanced Metering Infrastructure (AMI)

One area of critical importance to the security of the modernized grid is cryptography. Cryptographic techniques are used to ensure confidentiality, non-repudiation, and authentication. In the advanced metering infrastructure (AMI) the smart meters include multiple symmetric and/or asymmetric key pairs. With the deployment of millions of smart meters, cryptographic key management for millions of keys is a critical technical area for utilities.

The overall objective of this research project was to identify the design principles that are applicable to AMI and the management of cryptographic keys. Designing and implementing effective cryptographic key management schemes is a research area that requires the input from utilities and the cryptography community. The deliverable for this project was *Cryptographic Key Management (CKM) Design Principles for the Advanced Metering Infrastructure (AMI),* EPRI Technical Update 1024431 published in 2012.

6. Publications

All the NESCOR documents are available at: www.smartgrid.epri.com/nescor.aspx. The publications are listed in chronological order. All the EPRI reports may be accessed at: www.epri.com.

1. NESCOR, *Smart Energy Profile (SEP) 1.x Summary and Analysis*, October 31, 2011.
2. NESCO/NESCOR, *NESCO/NESCOR Common TFE Analysis: CIP-007 R5.3 Password Complexity*, 2011.
3. *CIPv5 NESCOR/NESCO/EPRI Comments*, January 2012.
4. *NESCOR/NESCO Comment Submission for the Second Version of the NERC CIP Version 5 Draft Documents*, May 2012.
5. EPRI, *Cyber Security Strategy Guidance for the Electric Sector,* Technical Update 1025672, May 2012.
6. NESCOR, *Wide Area Monitoring, Protection, and Control (WAMPAC): Standards for Cyber Security Requirements*, October 2012.
7. EPRI, *Network Security Management for Transmission Systems*, Technical Update 1024421, December 2012.
8. EPRI, *Draft Risk Assessment Processes*, Technical Update1024422, December 2012.
9. EPRI, *Risk Mitigation Strategies*, Technical Update1024423, December 2012.
10. EPRI, *Security Architectures for Integrating Distributed Energy Resources into the Grid*, Technical Update 1024425, December 2012.
11. EPRI, *Assessment of Technology Used to Protect the Privacy of Energy Usage Data*, Technical Update 1024426, December 2012.
12. EPRI, *Advanced Metering Infrastructure Security Objects,* Technical Update 1024427, December 2012.
13. EPRI, *Cryptographic Key Management (CKM) Design Principles for the Advanced Metering Infrastructure (AMI)*, Technical Update 1024431, November 29, 2012.
14. NESCOR, *Cyber Security for DER Systems,* Version, 1.0, July 2013.
15. NESCOR, *NESCOR Guide to Penetration Testing for Electric Utilities,* Version 3, July 2013.
16. NESCOR, *Analysis of Selected Electric Sector High Risk Failure Scenarios*, September 2013.
17. NESCOR, *Attack Trees for Selected Electric Sector High Risk Failure Scenarios*, September 2013.
18. EPRI, *Network System Management: End System Related IEC 62351-7 Object Definitions*, Technical Update, 3002000373, December 2013.
19. EPRI, *Guidelines for Planning an Integrated Security Operations Center,* Technical Update 3002000374, December 2013***.***
20. EPRI, *Lemnos Implementation Guide for IPSec, Device Configuration Examples,* Technical Update 3002000375, December 2013.
21. EPRI, *Framework for Grading Procurement Requirements for Power Delivery Systems*, Technical Update 3002001041, December 2013.
22. EPRI and DOE, *Integrating Electricity Subsector Failure Scenarios into a Risk Assessment Methodology,* Technical Update 3002001181, December 2013. (The document is available on the DOE website.)
23. NESCOR, *NESCOR Failure Scenario Toolkit*, June 2014.
24. NESCOR, *NESCOR Failure Scenarios and Impact Analyses*, V2.0, June 2014.
25. NESCOR, *NESCOR Guide to Vulnerability Assessment for Electric Utility Operations Systems*, Version 1.0, June 2014.
26. NESCOR, *NESCOR Common Vulnerabilities and Mitigations Mapping*, June 2014.

7. Presentations

1. NESCOR briefing to the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection Committee (CIPC) in 2011

2. NESCOR briefing to the UNITE Security Officers Meeting in 2011

3. Sandia National Lab – Albuquerque NM (Presentation to Staff Scientists (January 2011)

4. Edison Electric Institute EAC Group of CIOs in Washington DC (March 2011)

5. Queens University – Belfast Conference on Cybersecurity (March 2011)

6. UNITE Webcast on CyberSecurity (March 2011)

7. The principal investigator participated as a member of the Advisory Committee in the DOE led Electric Sector Cyber Security Risk Management Maturity Initiative. She is representing NESCOR. The document, *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)*, Version 1.0, was published May 31, 2012.

8. Penetration Testing Presentations: UtiliSec developed a 2-5 day, hands-on training course using the methodology and tasks presented in the NESCOR Guide to Penetration Testing. This course is currently being offered through the SANS Institute and Black Hat.
   Training given at:
   1. Distributech (January, 2013 in San Diego)
   2. SANS SCADA Summit (February, 2013 in Florida)
   3. Dakota State University (March, 2013 in Madison, SD)
   4. SANS ICS Training (June, 2013 in Houston, TX)
   5. Oak Ridge, Tennessee in March 2013

9. Briefing at the SmartSec Europe 2014 workshop in Amsterdam on the failure scenarios[3].

10. Briefing to the intelligence community on the failure scenarios in February 2014.

11. EPRI conducted annual workshops in 2011, 2012, and 2013 that highlighted the work being performed by the TWGs and the cost share projects being executed by EPRI. In addition, keynote speakers gave presentations on current cyber security issues. Finally, each workshop included a working session for the TWGs. The TWGs held regular telecons so this was an opportunity to have a face-to-face meeting with the various participants. All the NESCOR sub-recipients and several representatives from DOE attended.

[3] The trip was sponsored by EPRI and not part of the cost share tasks.

8. Sustainability of the NESCOR Project

One of the important goals of the NESCOR project was to continue the work beyond the period of the award. EPRI has established a share point site and ported all the deliverables that were posted on the EnergySec website to this new site. The URL for the website is: https://nescor.sharepoint.com/TWG2/_layouts/15/start.aspx#/. Currently there are over 60 individuals with access to the site. Also, all the NESCOR documents are available at the EPRI site: www.smartgrid.epri.com/NESCOR.aspx

EPRI is continuing to work on the failure scenarios, particularly in the generation sector. The original document did not include them.

As stated in the original funding announcing, “It is expected that the organization will become self-sustaining through the energy sector partnership in future years.” Also, in the assessment criteria, “Credibility of long-term plan for continuation, self-sustainment, and lasting impact of the organization beyond the project period.” In response to this, EPRI established several cost share projects that are directly related to and build upon the NESCOR projects. These EPRI projects are described above. Also included in this report are the “future activities” for many of these projects.