Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

SGIG Cyber Security Program Review Process

A. DAVID MCKINNON, PH.D.

Cyber Security Group, National Security Directorate

TCIPG Industry Workshop 2014

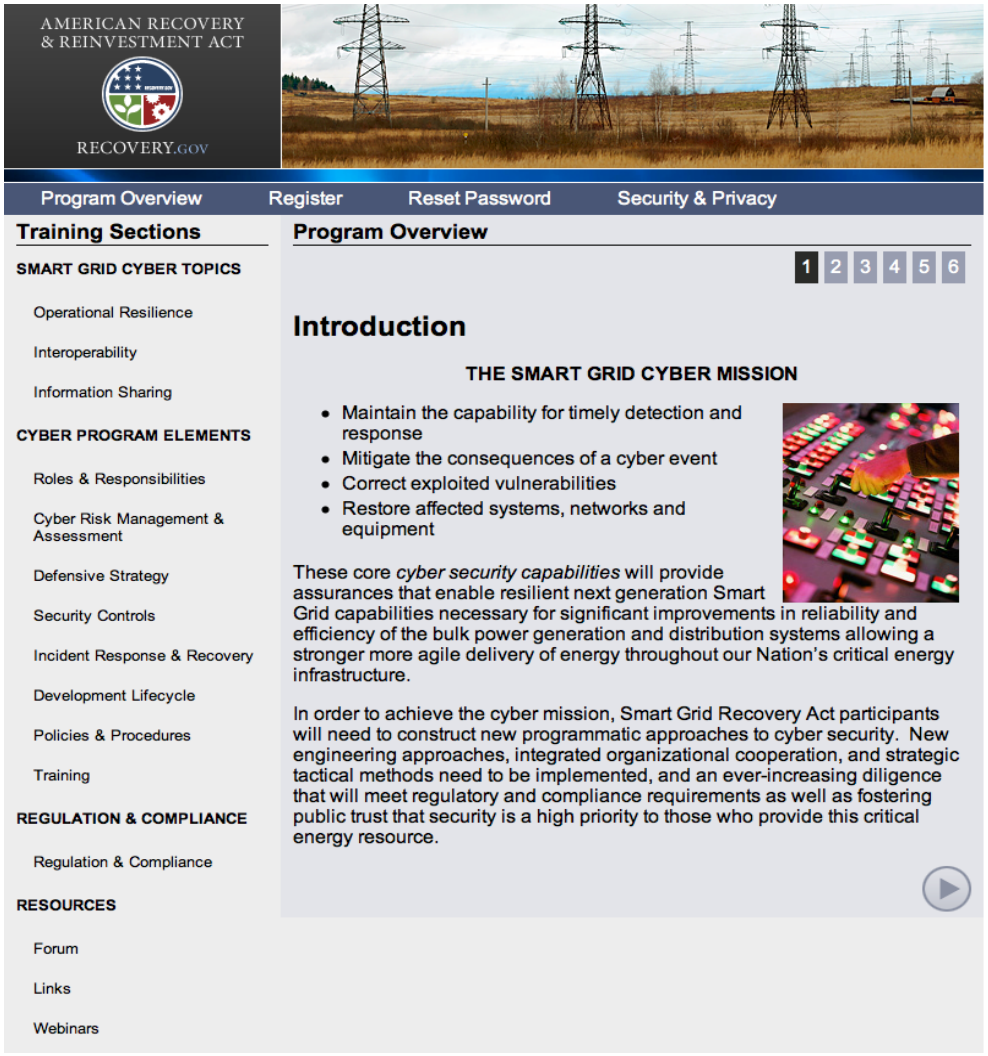
SGIG Cyber Security Program Overview

- Smart Grid Investment Grant (SGIG) was funded by the 2009 ARRA
  - 99 Grants awarded
  - $3.4B of federal funding, matched by $4.4B of private sector funding
- Cyber security was “built in”
  - FOA required that each proposal address cyber security
  - Each awardee had to submit a cyber security plan (CSP) for review and approval
- DOE established a cybersecurity subject matter expert (CS-SME) team
  - Team consisted of leading cyber security experts from PNNL, ANL, CMU SEI, and private industry
  - CS-SME team members joined the DOE technical project officer (TPO) on their annual site visits
  - CS-SME team conducted several outreach activities

Cyber Security Requirements (DE-FOA-0000058)

- Submitted Project Plans are also required to include a section on the technical approach to cyber security.
- The technical approach to cyber security should include:
  - A summary of the cyber security risks and how they will be mitigated at each stage of the lifecycle (focusing on vulnerabilities and impact).
  - A summary of the cyber security criteria utilized for vendor and device selection.
  - A summary of the relevant cyber security standards and/or best practices that will be followed.
  - A summary of how the project will support emerging smart grid cyber security standards.
- DOE intends to work with those selected for award but may not make an award to an otherwise meritorious application if that applicant cannot provide reasonable assurance that their cyber security will provide protection against broad based systemic failures in the electric grid in the event of a cyber security breach.

www.ARRASmartGridCyber.net



- Online information resource for SGIG & SGDP cyber security
  - Overview of baseline cyber security principles
  - Guidance on cyber security plan development and execution
  - References to cyber security standards and regulations
- Prescriptive "templates" for cyber security plans were ***not*** provided

99 Cyber Security Plans

- Cyber security—one size does ***NOT*** fit all
  - Grant awards varied from $1M to $200M
  - Technologies varied
    - Electric transmission systems
    - Electric distribution systems
    - Advanced metering infrastructure (AMI)
    - Customer systems
    - Cross-cutting deployments
  - Awardees used their own internal processes and templates
- DOE technical project officers (TPO) forwarded each project's cyber security plans to the CS-SME team
- Each plan was independently reviewed by two CS-SMEs
  - Initial reviews were conducted by all team members
  - Secondary reviews were performed by a "QC" subteam member

Cyber Security Plan Reviews

- Strong cyber security plans included:
  - Cyber security risks and how they will be mitigated at each stage of the lifecycle (focusing on vulnerabilities and impact)
  - Cyber security criteria utilized for vendor and device selection
  - Relevant cyber security standards and/or best practices to be followed
  - Plans for supporting emerging smart grid cyber security standards
- Cyber security plans also had to address the adequacy of their technical approach for addressing interoperability and cyber security
  - Ensuring confidentiality, integrity, availability
  - Secure logging, monitoring, alarming, and notification
  - Demonstrable evidence of the effectiveness of cyber security controls
- Inadequate cyber security plans were revised and resubmitted
  - CS-SME team frequently held project-specific teleconference calls
    - Interactive discussion quickly resolved issues
    - Many awardees did not have prior experience writing cyber security plans

244 Site Visits

- SGIG project reviews included cyber security
  - CS-SMEs traveled with the DOE review team
  - Cyber security was a formal topic on the agenda
- Site visits were conducted 2011-2013
  - 2011-2012: on-site visits
  - 2013: on-site, virtual, or off-line visits at the discretion of the DOE TPOs
- Guidance was provided to each site prior to the annual site visits
- Focus on demonstrable evidence
  - Were project-specific risks being identified and addressed?
  - Were implemented cyber security controls adequate?
  - No prescribed format for how “evidence” was to be provided
- Site assessment visit report
  - 13 requirements derived from FOA were assessed
  - Scale: **meets**, **meets most**, & **does not meet** FOA requirements

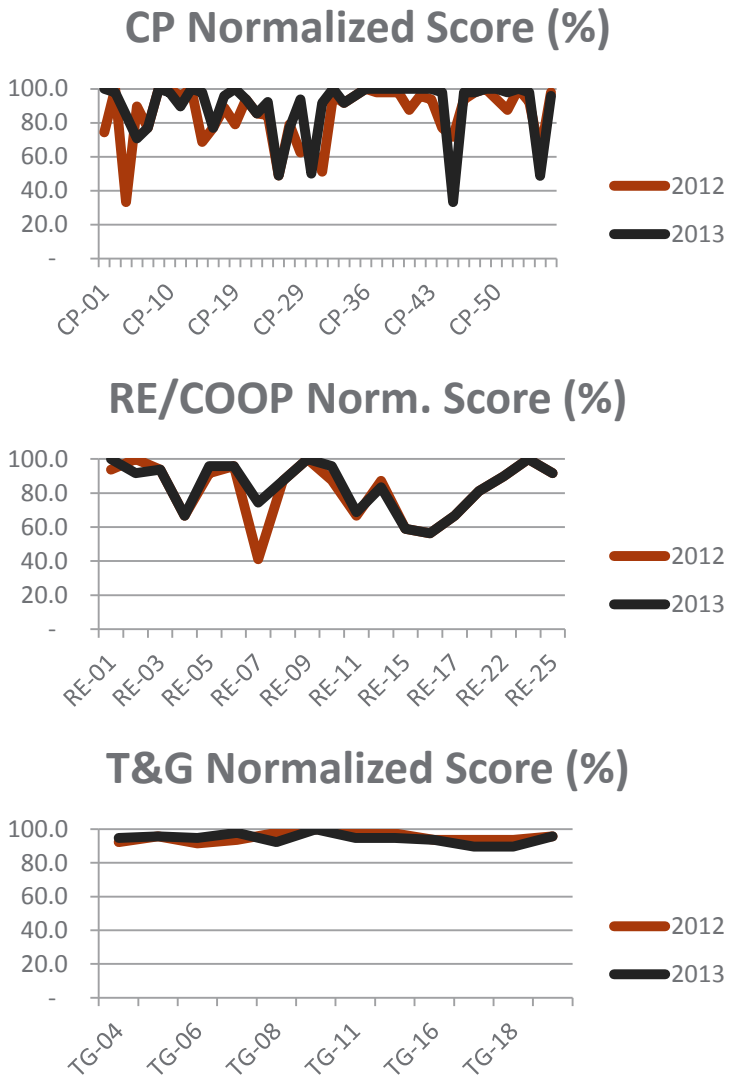
Cyber Security Impact

- Cyber security was a FOA requirement
  - Senior-level management approved cyber security plans
  - Cyber security was a ***funded*** requirement
- Each project was able to focus on *their* specific risks
- Awardees and the CS-SMEs built close working relationships
- Smart grid cyber security information exchanges
  - Chicago (August 2011) & Washington, D.C. (December 2012)
  - Utilities met & exchanged cyber security best practices

- Many anecdotal stories of utilities implementing new and/or improved cyber security practices
  - Enhanced staffing, training, policies, tools, etc.

Cyber Security Impact, continued

- CS-SME team assessment
  - Based upon a weighted scoring of each site assessment report
    - 13 questions, **Green**/**Yellow**/**Red**
  - Projects were grouped by category
    - Cities/Public Utility Districts (CP)
    - Rural Electric Cooperatives (RE/COOP)
    - Transmission/Generation (T&G)
  - Compared 2012 and 2013 results
- CP had the largest score improvement
- RE/COOP had the 2nd best improvement
- T&G improved the least
  - *Caveat*: T&G projects had the best overall scores



SGIG Cyber Security Conclusions

- FOA requirement for cyber security was a key enabler
  - Utilities were able to *build-in* in cyber security
  - DOE facilitated across-the-board cyber security improvements
- Project staff, DOE TPOs, and the CS-SME team built strong and trusted working relationships
- Cyber security plans focused and enhanced cyber security efforts
  - Each project focused on their specific risks
  - Cyber security plans are “living” documents
  - Approval by senior-level management provided accountability