Cyber Security Review Summary for the Smart Grid Investment Grants

Jeff Dagle, PE
Chief Electrical Engineer
Advanced Power & Energy Systems
Pacific Northwest National Laboratory

October 13, 2011

Pacific Northwest
NATIONAL LABORATORY

Cyber Security *Critical* to Smart Grid Success

Cyber security requirements of the Recovery Act grant funding:

- Organized interagency group (DOE, NIST, FERC, DHS, others) for development of cyber security requirements in the funding opportunity announcement (FOA)
- Cyber security was a factor in evaluating the grant proposals
- Cyber security plans were required, and evaluated by a team of subject matter experts
- Site visits underway with all smart grid investment grant recipients to review cyber security plan implementation

> ***"DOE may not make an award to an otherwise meritorious application if that application cannot provide reasonable assurance that their approach to cyber security will prevent broad based systemic failures in the electric grid in the event of a cyber security breach."***
>
> **Smart Grid FOA**

Pacific Northwest
NATIONAL LABORATORY

Cyber Security Plan Requirements

- Evaluate risks and how they will be mitigated at each stage of the lifecycle (focusing on vulnerabilities and impact)
  - Methodology and results, considering mission impacts
- Criteria for vendor and device selection
- Summarize relevant cyber security standards and/or best practices that will be followed
- Upgradeability, both components and systems
- How the project will support emerging standards
- Evidence to demonstrate and validate the effectiveness of the cyber security controls
- Accountability

Site Visit Objectives

- Perform on site reviews of all smart grid investment grant recipients to ensure adequacy of planning and implementation and that the projects are on track for a successful installation
  - Primary focus of a site visit is to review demonstrable evidence that the cyber security plan is being implemented as approved by DOE
  - Additionally, learn from the grantees' experience to capture best practices, implementation challenges, and lessons learned that may be shared with others
  - Provide support to projects on cyber security issues and concerns

Recommendation

Organizational Accountability

- Have well-defined chain of accountability with clearly defined roles and responsibilities
  - Organizational commitment to the process
- Apply architectural review process throughout project lifecycle
  - Policies addressing the testing, validation, and integration of security controls, technologies, and upgrades
  - Reassess risk to services and infrastructure as changes are made
- Regular meetings between management and cyber security experts to show direct support and accountability
  - All principal players with project responsibility should be actively involved with the implementation and periodic review of the cyber security plan
  - Maintain an organization chart denoting cyber security responsibilities and chain of command that traverses contractors, field crews and management
- Interactions between the grant recipient and DOE should confirm the intent of the grant recipient to provide the necessary resources to fully integrate cyber security within the system

Recommendation

Risk and Vulnerability Assessment

- Execute risk, vulnerability and mitigation processes and periodically review for changes
  - Adhere to existing and emerging standards and best practices
  - Include testing to confirm specifications
  - Involve vendors and consider third party support
- Particular attention to external connections, interconnection between different vendors' systems, third party service providers, etc.
- Disable unneeded services and/or connectivity
- Understand gaps in the cyber security plan and identify required actions to implement additional security controls, as appropriate
- Follow published industry and government cyber security standards, where applicable
- Follow best practices for physical security
  - e.g., badge reader system, check-in/out sheets, cameras, etc.

Recommendation

Protection, Response, & Recovery

- Cyber Security Incident Response Team
  - Address and monitor concerns associated with cyber security events
- Incident Response and Recovery strategy should include a comparative review of logs and reports prior to mitigation with those after mitigation
- Limiting vendor connectivity to critical systems
  - Selectively allow connectivity on request, restrict with time limits and other security controls
- Identify backup processes in event automation or patching creates operational problems
- Limit connections to operational systems as “read only” if practical
- Implement security policies for laptop computers used for control and non-control purposes

Sources of Cyber Security Knowledge and Help

- DOE ARRA cyber security website:
  - **https://www.arrasmartgridcyber.net /**
- Responsible staff including management should become familiar with the smart grid technologies being deployed
  - Training for field personnel should include cyber security awareness as well as configuration and maintenance of cyber security architecture and controls
- Participate in various smart grid information-sharing groups and conferences, workshops, webinars, and committees
  - Participate with NIST, NERC, and other standards development activities
  - Regional and/or local engagement
- Utilize DHS Guidelines on “Cyber Security Procurement Language for Control Systems”
- NRECA website:
  - https://groups.cooperative.com/smartgriddemo/public/CyberSecurity/Pages/default.aspx