Interim Technology Performance Report 1

PROJECT BOEING SGS

Contract ID: DE-OE0000191

Project Type: Regional Demonstration

Revision: V2

Company Name: The Boeing Company

December 10, 2012

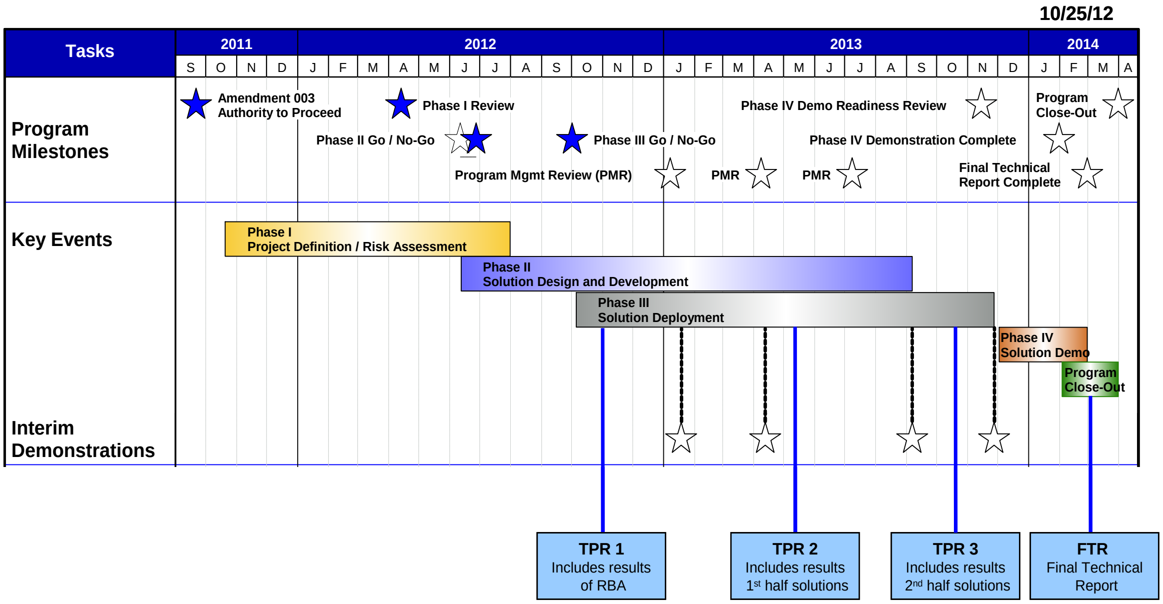
TABLE OF CONTENTS

1. Introduction

This document represents the first of three Interim Technology Performance Reports for the Project Boeing SGS Regional Demonstration. Under a cooperative agreement with the Department of Energy, Boeing and its partner, PJM Interconnection, have teamed to demonstrate advanced technology solutions focused on cyber security in an energy management environment on the US regional power grid. The team is employing a combination of processes, techniques and technologies that have been successfully implemented in the commercial, defense, and intelligence communities to identify, mitigate and continuously monitor cyber-security risks to critical systems. The successful completion of the project's objectives will benefit residents throughout the entire region and provide future opportunity to scale and replicate across the energy grid.

This Technology Performance Report, identified as TPR1 on the Project Integrated Schedule shown in Figure 1, covers the critical Phase I Risk Assessment and the initial portion of the Phase II Solution Design and Development. Solution development and deployment is being undertaken in a serial-parallel fashion consisting of multiple iterations of specific candidate solutions designed to mitigate vulnerabilities uncovered during the Phase I Risk Assessment.

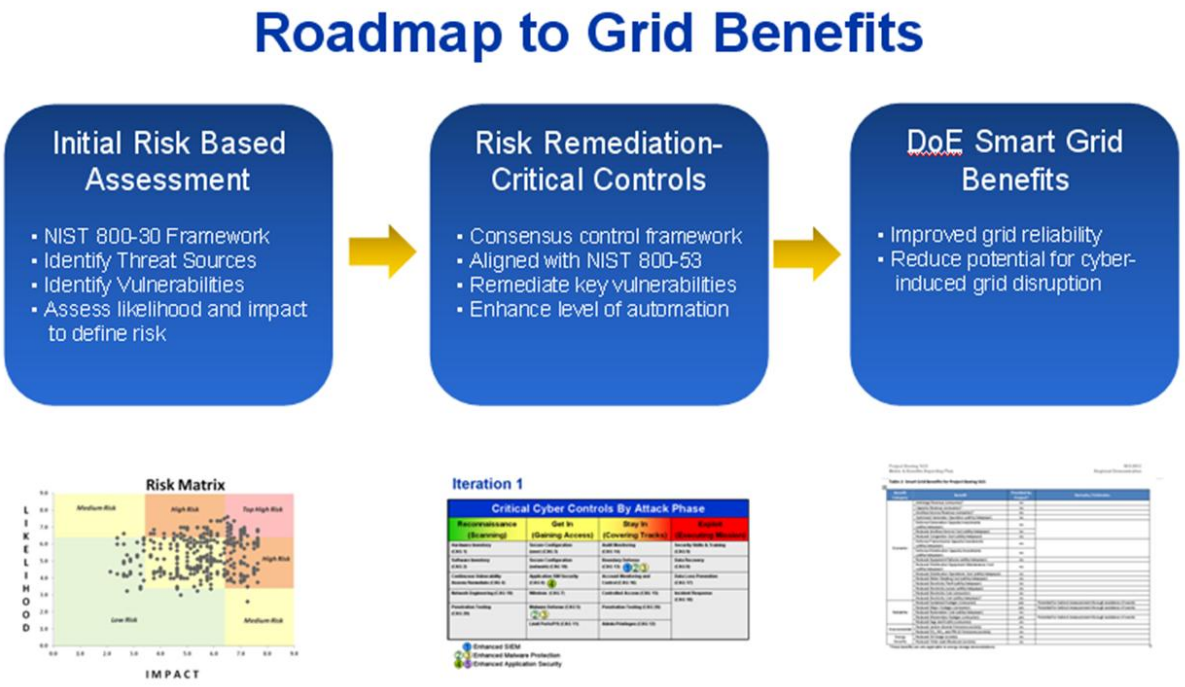
Figure 1- Project Boeing SGS Integrated Schedule



2. Grid Level Benefits Overview

Enhanced protection of critical grid infrastructure from potential cyber-induced harm is a fundamental societal benefit realized through the execution of this project. Assessing the discrete cyber-security risk to the electrical grid as a whole or even as a control region such as that represented by PJM's control territory is beyond the scope of this project. However, by focusing the project's cyber-security risk-based assessment on PJM's critical systems, subsequent remediation efforts (both project funded and off-project funded) will ultimately address those vulnerabilities that are most critical to providing an improved level of cyber-security for the electrical grid. The project team has completed the Phase I Risk Based Assessment of PJM's critical systems, the results of which will guide the subsequent solution development, deployment, and demonstration phases of the project.

Figure 2- Project Boeing SGS Linkage to Smart Grid Benefits



Roadmap to Grid Benefits

Initial Risk Based Assessment

- NIST 800-30 Framework
- Identify Threat Sources
- Identify Vulnerabilities
- Assess likelihood and impact to define risk

Risk Remediation-Critical Controls

- Consensus control framework
- Aligned with NIST 800-53
- Remediate key vulnerabilities
- Enhance level of automation

DoE Smart Grid Benefits

- Improved grid reliability
- Reduce potential for cyber-induced grid disruption

Risk Matrix
LIKELIHOOD
IMPACT
Medium Risk
High Risk
Top High Risk
High Risk
Low Risk
Medium Risk
Iteration 1
Critical Cyber Controls By Attack Phase
Reconnaissance (Scanning)
Get In (Gaining Access)
Stay In (Covering Tracks)
Exploit (Executing Mission)
Enhanced SIEM
Enhanced Malware Protection
Enhanced Application Security

The key activities and outcomes of the Cyber-Security Risk Assessment are depicted graphically in the first block of Figure 2. The risk assessment culminated in a risk matrix derived from the pairing of likely threat actors (sources) to identified critical asset vulnerabilities. The second block of Figure 2 depicts cyber-security control remediation directed at identified vulnerabilities. Solution development and deployment candidate activities have already commenced and the remaining phases of the project will be focused on these activities. The final block depicts the Smart Grid Benefits of improved reliability and reduced potential for cyber-induced grid disruption that result both directly, from activities funded as a result of this project, and indirectly, from activities funded outside of this project that result from findings of the of the project's risk based assessment. Additional indirect benefits may also be realized across the electrical sector through opportunities to replicate the processes, tools, techniques and solutions developed on this Smart Grid demonstration project.

3. Cyber Security Risk Assessment

A fundamental first step of the project was to determine cyber security risks to the PJM network / information system that supports the regional Bulk Electric System (BES) operated by PJM. Risk management of the PJM information system is essential to protecting cyber assets and thus PJM's overall mission. The risk management process identifies risks, assesses risks, and then takes steps to reduce risk to an acceptable level. This section summarizes the completed Phase I Risk Assessment. The scope of this assessment was constrained to high-value PJM information systems and provides a baseline for remediation efforts.

3.1 Methodology

The risk assessment adhered to NIST Special Publication 800-30 (Risk Management Guide for Information Technology Systems) by executing each of the eight defined steps while tailoring step details for the energy sector.

Step 1 determined the portion of the PJM system to be assessed which resulted in focusing the data collection and assessment to the PJM Identified high-value systems and followed by a further narrowing to three high-value systems and their support systems.

Step 2 defined seven potential human threat-sources in two groupings: *external* (nation-state, terrorist, industrial spy/organized crime, hacktivist/hacker) and *internal* (employee, member, and vendor). The assessment focused on human threat-sources as opposed to natural and environmental threat-sources due to resource constraints and because PJM policies, standards and procedures already mitigate natural and environmental threats.

Step 3 defined applicable vulnerabilities as the 52 vulnerability categories and associated definitions in NISTIR-7628 (Guidelines for Smart Grid Cyber Security, Vol 3). This set is considered energy sector-applicable and comprehensive because it includes vulnerabilities related to policy, software/firmware, platforms, and networks. In addition, step 3 identified specific PJM vulnerabilities which were also associated with each of the 52 categories and applied in following steps.

Step 4 identified the current PJM security controls that apply to high-value systems. These controls were identified within PJM's policy, standards, and procedure documents (70 of 140 were considered applicable and reviewed). Each PJM control was associated with one of the 205 controls in the well-known standardized set from NIST SP800-53. Each standardized control was associated with one or more vulnerability categories in Step 3.

It is the 364 (7x52) pairs of threat-sources and vulnerabilities from steps 2 and 3 and associated controls in step 4 that formed the threat space for the risk evaluation.

Step 5 assigned a likelihood rating to each threat (a combination of a threat-source and vulnerability category mitigated by known controls). At the highest level, the likelihood rating is a subjective judgment of how likely a threat is to be successful against one of the three high-value systems. A modified Open Web Application Security Project (OWASP) methodology was used to determine the likelihood rating (range 0-9) where larger values represent a more likely occurrence.

Step 6 assigned an impact rating to each threat. Similar to the likelihood rating, the impact rating is an estimate of the likely damage if the threat was successful against one of the three high-value systems. A modified OWASP methodology was also used to determine the impact rating (range 0-9).

Step 7 uses the likelihood rating (step 5) and impact rating (step 6) as an indicator of risk for each threat. This assessment has categorized risk into four levels: low, medium, high, and top high.

Step 8 provides an analysis of PJM-specific vulnerabilities and their relationship to risks.

3.2 Use of Automated Tools

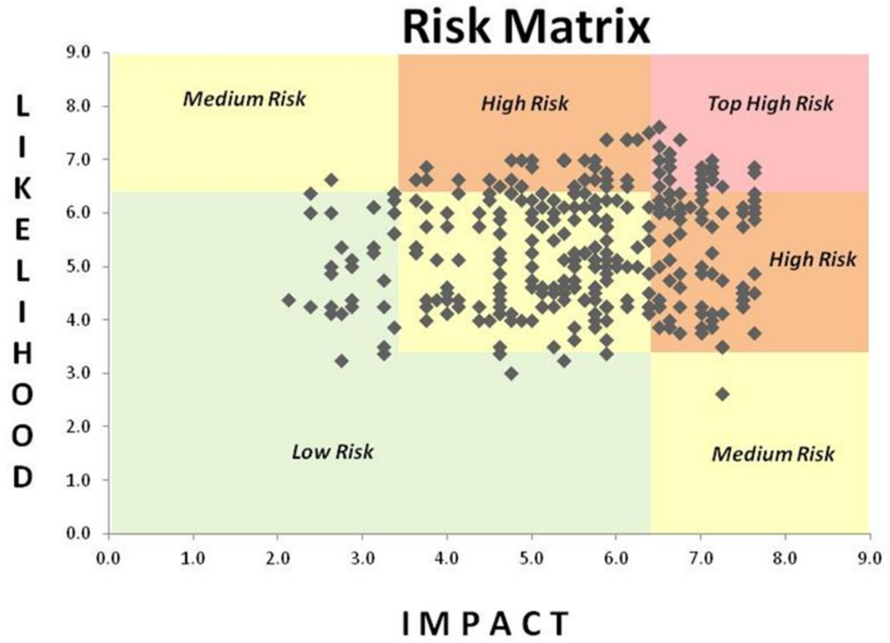
Along with information gathered by Boeing during interviews with PJM Subject Matter Experts (SMEs), the deployment of automated security analysis tools contributed to the system characterization (Step 1) and vulnerability identification (Step 3) steps. For example one such tool automatically maps network access by analyzing network device configurations, including routers, firewalls and load-balancers and then correlates network access with the findings of vulnerability assessment scans to help make better network security decisions. Another valuable tool, the Boeing Enterprise Network Security (ENS) tool was also used to help identify vulnerabilities (Step 3) in the PJM information system. ENS detects malicious activity occurring within the network during any of the four phases of the typical threat life-cycle:

- Phase 1 – **Reconnaissance**: the attacker characterizes the targeted network/information system both from an external and internal viewpoint
- Phase 2 – **Intrusion**: malware attempts to compromise specific elements of the network/information system
- Phase 3 – **Communications Establishment**: malware will callback from a compromised internal host to an external command and control server
- Phase 4 – **Suspicious Data-In-Motion/Exfiltration**: unauthorized data is moved either internal to or exfiltrated from the network/information system

3.3 Risk Evaluation

After analyzing the impact and likelihood values for all potential threats, twenty-six (26) Top High risks were identified. Application security vulnerabilities show up as dominant with malware protection, integrity checking, and security architecture and design vulnerabilities to a lesser extent. Few threat-vulnerability pairs are indicated in the “Low Risk” category due to the project focus on critical systems.

Figure 3- Risk Assessment Threat-Vulnerability Risk Matrix



Overall, it was observed that PJM currently maintains a robust cyber security posture as witnessed by the following:

- A reasonable and consistent security training program
- A strong base of policies, standards, and procedures
- A good basic set of cyber monitoring tools
- A threat-aware, vigilant, skilled security/network staff

4. Remediation and Controls

Guided by the risk assessment findings, the project team has begun specific solution development activities. While specific vulnerabilities (and associated risks) identified during the risk assessment will not be discussed in this report, general solution candidates for the first iteration of remediation and control response will be presented within a common control framework.

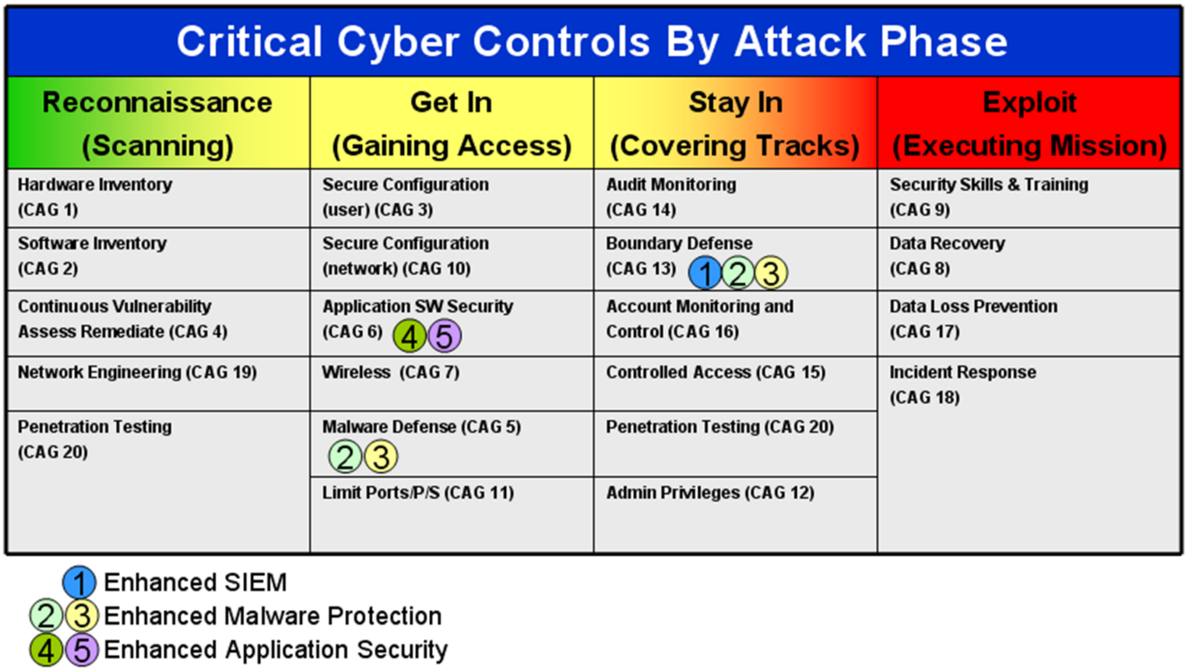
4.1 20 Critical Controls for Effective Cyber Defense

The 20 Critical Controls for Effective Cyber Defense is a widely recognized framework of security controls, cooperatively developed between the US Government and industry subject matter experts, to establish a prioritized baseline of information security measures and controls that can be applied consistently across federal and commercial environments. Please refer to www.sans.org/critical-security-controls/ for complete reference and most recent version as maintained by the SANS Organization including mappings to NIST Special Publication 800-53 Priority 1 Controls and NSA Manageable Network Plan content.

4.2 Iteration 1 Design and Development Candidates

The project has identified five initial design and development candidates for the first of several remediation cycles. Figure 4 illustrates the general controls areas affected and indicates in which phases of the cyber threat lifecycle where security controls will be improved.

Figure 4- Iteration 1 Solution Candidates by Threat Phase and Control Area



Critical Cyber Controls By Attack Phase

Reconnaissance (Scanning)	Get In (Gaining Access)	Stay In (Covering Tracks)	Exploit (Executing Mission)
Hardware Inventory (CAG 1)	Secure Configuration (user) (CAG 3)	Audit Monitoring (CAG 14)	Security Skills & Training (CAG 9)
Software Inventory (CAG 2)	Secure Configuration (network) (CAG 10)	Boundary Defense (CAG 13) ①②③	Data Recovery (CAG 8)
Continuous Vulnerability Assess Remediate (CAG 4)	Application SW Security (CAG 6) ④⑤	Account Monitoring and Control (CAG 16)	Data Loss Prevention (CAG 17)
Network Engineering (CAG 19)	Wireless (CAG 7)	Controlled Access (CAG 15)	Incident Response (CAG 18)
Penetration Testing (CAG 20)	Malware Defense (CAG 5) ②③	Penetration Testing (CAG 20)	
	Limit Ports/P/S (CAG 11)	Admin Privileges (CAG 12)	

① Enhanced SIEM
②③ Enhanced Malware Protection
④⑤ Enhanced Application Security

The 20 Critical Controls should be viewed more as “control categories” given that an organization as sophisticated as PJM already has a very large number of very specific controls in place in each of the 20 designated categories. The intent of this project is to direct resources to those areas with the potential to offer the largest degree of security return for the given investment applied.

Collectively, the five Iteration 1 candidates fall into three general areas of interest.

- **Enhanced Security Incident and Event Management (SIEM)**

  The intent of this candidate is to enhance an already effective SIEM system through configuration changes and visibility improvements to address both general operational efficiencies and specific risk based assessment findings.

- **Enhanced Malware Protection**

  Several candidate solutions are in work in the area of malware protection to 1) address specific remediation of risk based assessment findings and 2) implement leading edge technology to demonstrate significant improvements in malware threat detection capability.

- **Enhanced Application Security**

  Several iteration candidates are in work that fall under the general topic area of Application Security, completion of which is intended to address issues more systematically and establish a framework going forward to enhance overall effectiveness of the Application Security program already in place at PJM.

5. Summary and Next Steps

The Project Boeing SGS team has completed the Phase 1 risk-based cyber security assessment of PJM’s critical cyber assets. The assessment results form the basis of all subsequent solution design and development activities undertaken within the scope of this project and may guide efforts undertaken outside the scope of this project as well.

The first set of solution candidates has been determined and development and deployment of those solutions is currently underway. Candidate solutions for follow-on design and development iterations have also been identified and are currently under review for deployment in the follow-on iteration cycles.

Subsequent Interim Technology Performance Reports will address the project team’s ongoing development and deployment iterations and the remediation activities included in each. The Final Project Report will include a reassessment of the cyber security risk matrix capturing the total realized risk reduction to PJM’s critical systems resulting from this Smart Grid demonstration project.

Appendix A- Smart Grid Benefit Impact Areas

Benefit Category	Benefit	Provided by Project?	Remarks / Estimates
Economic	Arbitrage Revenue (consumer)*	no	
	Capacity Revenue (consumer)*	no	
	Ancillary Service Revenue (consumer)*	no	
	Optimized Generator Operation (utility/ratepayer)	no	
	Deferred Generation Capacity Investments (utility/ratepayer)	no	
	Reduced Ancillary Service Cost (utility/ratepayer)	no	
	Reduced Congestion Cost (utility/ratepayer)	no	
	Deferred Transmission Capacity Investments (utility/ratepayer)	no	
	Deferred Distribution Capacity Investments (utility/ratepayer)	no	
	Reduced Equipment Failures (utility/ratepayer)	no	
	Reduced Distribution Equipment Maintenance Cost (utility/ratepayer)	no	
	Reduced Distribution Operations Cost (utility/ratepayer)	no	
	Reduced Meter Reading Cost (utility/ratepayer)	no	
	Reduced Electricity Theft (utility/ratepayer)	no	
	Reduced Electricity Losses (utility/ratepayer)	no	
	Reduced Electricity Cost (consumer)	no	
	Reduced Electricity Cost (utility/ratepayer)*	no	
Reliability	Reduced Sustained Outages (consumer)	yes	Potential for indirect measurement through avoidance of events
	Reduced Major Outages (consumer)	yes	Potential for indirect measurement through avoidance of events
	Reduced Restoration Cost (utility/ratepayer)	no	
	Reduced Momentary Outages (consumer)	yes	Potential for indirect measurement through avoidance of events
	Reduced Sags and Swells (consumer)	no	
Environmental	Reduced carbon dioxide Emissions (society)	no	
	Reduced SO$_X$, NO$_X$, and PM-10 Emissions (society)	no	
Energy Security	Reduced Oil Usage (society)	no	
	Reduced Wide-scale Blackouts (society)	no	

*These benefits are only applicable to energy storage demonstrations.