Interim Technology Performance Report 2

PROJECT BOEING SGS

Contract ID: DE-OE0000191

Project Type: Regional Demonstration

Revision: V2

Company Name: The Boeing Company

Jun 11, 2013

TABLE OF CONTENTS

1. Contents

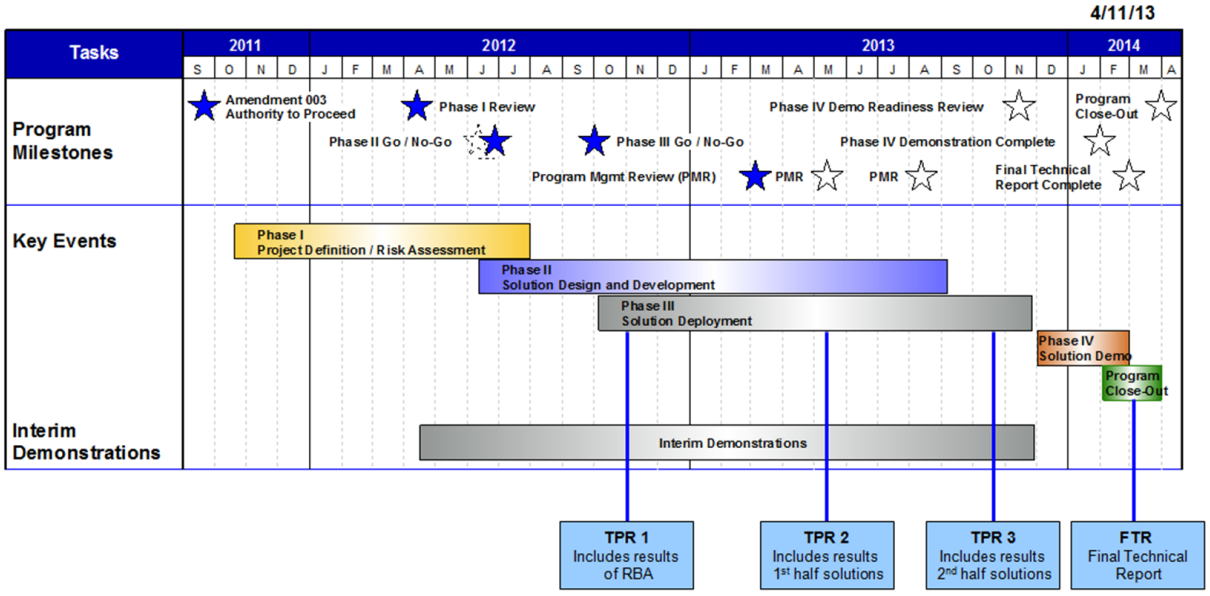
2. INTRODUCTION 3
3. ASSESSMENT REVIEW AND INITIAL REMEDIATION DETERMINATION 4
4. ENHANCED SECURITY INCIDENT AND EVENT MANAGEMENT (SIEM) 5
4.1 ENHANCED SIEM - PATH FORWARD 6
5. ENHANCED MALWARE ASSESSMENT 7
5.1 ENHANCED MALWARE ASSESSMENT- PATH FORWARD 7
6. ENHANCED APPLICATION SECURITY 8
6.1 ENHANCED APPLICATION SECURITY - PATH FORWARD ..... **ERROR! BOOKMARK NOT DEFINED.**
7. SUMMARY 9
APPENDIX A GRID LEVEL BENEFITS OVERVIEW 10

2. Introduction

This document represents the second 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 the reliability of the bulk electric system throughout the entire region and provide future opportunity to scale and replicate across the energy grid.

This Technology Performance Report, identified as TPR2 on the Project Integrated Schedule shown in Figure 1, covers initial portions of Phase II Solution Design and Development and Phase III Solution Deployment. Phases II and III are 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.

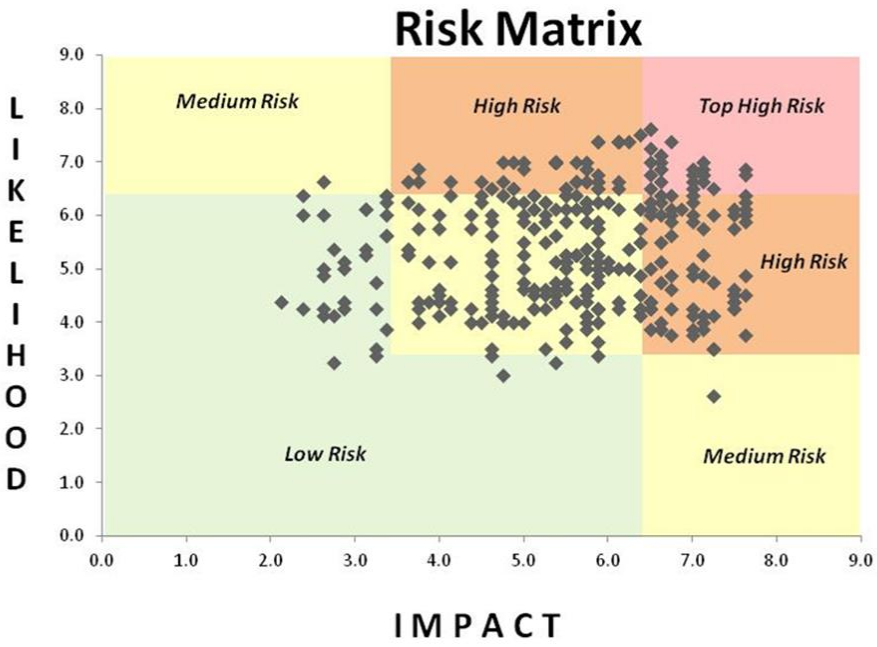
Figure 1- Project Boeing SGS Integrated Schedule



3. Assessment Review and Initial Remediation Determination

As detailed in TPR1, the Phase I Risk Based Assessment of PJM's high value information systems was undertaken and 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. Mapping potential threat actors to potential vulnerabilities resulted in the risk matrix shown in Figure 2. 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 2- Risk Assessment Threat-Vulnerability Risk Matrix



Guided by the risk assessment findings, the project team determined specific solution development activities with the potential to offer the largest degree of security return for the given investment applied. Initial solution candidates were identified under three categories:

- **Enhanced Security Incident and Event Management (SIEM)**
- **Enhanced Malware Protection**
- **Enhanced Application Security**

The following section provides an overview of developments, deployments and benefits seen to date from remediation efforts in these areas.

4. Enhanced Security Incident and Event Management (SIEM)

Enhancing the level of situational awareness provided by an integrated SIEM can result in highly cost effective security improvements. Ensuring that the SIEM is well integrated with all monitoring devices, event reports are well understood in context, and that operators are not overwhelmed with a large number of false or low priority events can significantly improve the value of an existing SIEM.

Initial SIEM solution development and deployment iterations have been focused on thorough identification and integration of all relevant monitoring devices on PJM high value systems and then achieving event correlation and reporting within their respective phase of the threat life cycle.
The life cycle of an Advanced Persistent Threat (APT) being defined as follows:

- **Phase 1 – Reconnaissance**: The period of time where the adversary is performing reconnaissance on your enterprise by doing port scans, social engineering, browsing external facing websites and servers, etc. In this period of time the adversary is also taking all the information gathered and is tailoring an attack to your defenses to achieve their objective.

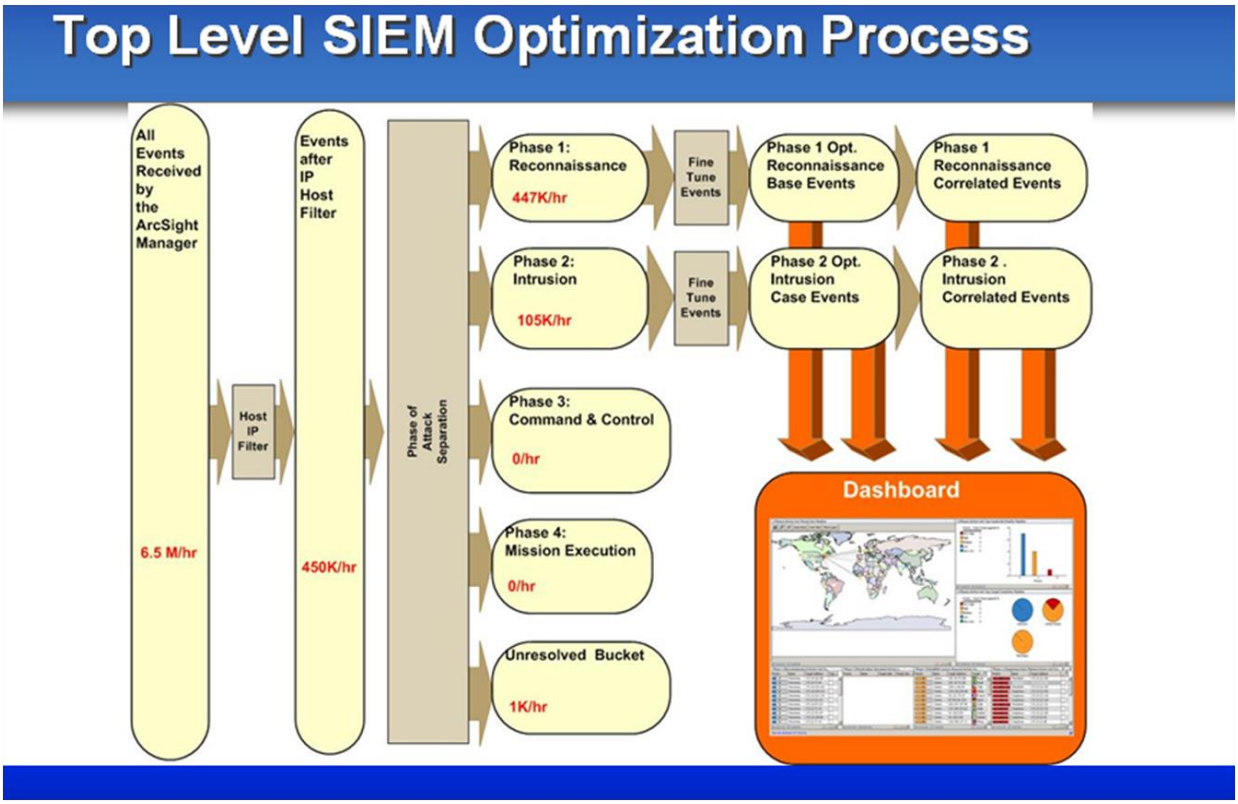
- **Phase 2 – Intrusion**: The period of time where the adversary is launching its attack in an attempt to gain access to your enterprise and your data. Examples of this include spear phishing attempts, launching zero day exploits, handing out "free" infected thumb drives at conferences, attempting to hack into a system remotely, etc. –Note: Up until this point in time, the victim is not compromised; the stage is set so that they can be compromised. Also in this period of time the attack delivered executes and finds out whether or not compromise could in fact occur. Not all exploits are successful. Once compromise occurs, privileges are escalated, additional code is downloaded from the remote adversary, initial communication is established with the adversary, etc.

- **Phase 3 – Command and Control Establishment**: The period of time where the adversary and the compromised system communicate regarding its mission. Activities in this phase will include beaconing, scanning the infected system, scanning other internal systems, downloading of additional instructions from command and control server, etc.
- **Phase 4 – Mission Execution / Data-In-Motion / Exfiltration**: The period of time where the adversary executes its mission through the internally compromised machine. This includes data exfiltration, data or system corruption, launching pivot attacks, etc.

By aligning the security dashboard to register events within a specific threat phase, a significantly enhanced level of situational awareness is achieved when potential cyber security events are detected. Remediation action determination and timeliness improvements enhance the overall resiliency of the system(s) under protection.

System operational efficiency will likewise benefit from the inclusion of event filtering into the optimization process which results in a security dashboard with significantly fewer, but more specifically targeted base events for evaluation. Figure 3 provides a top level view of the process.

Figure 3- SIEM Optimization Process



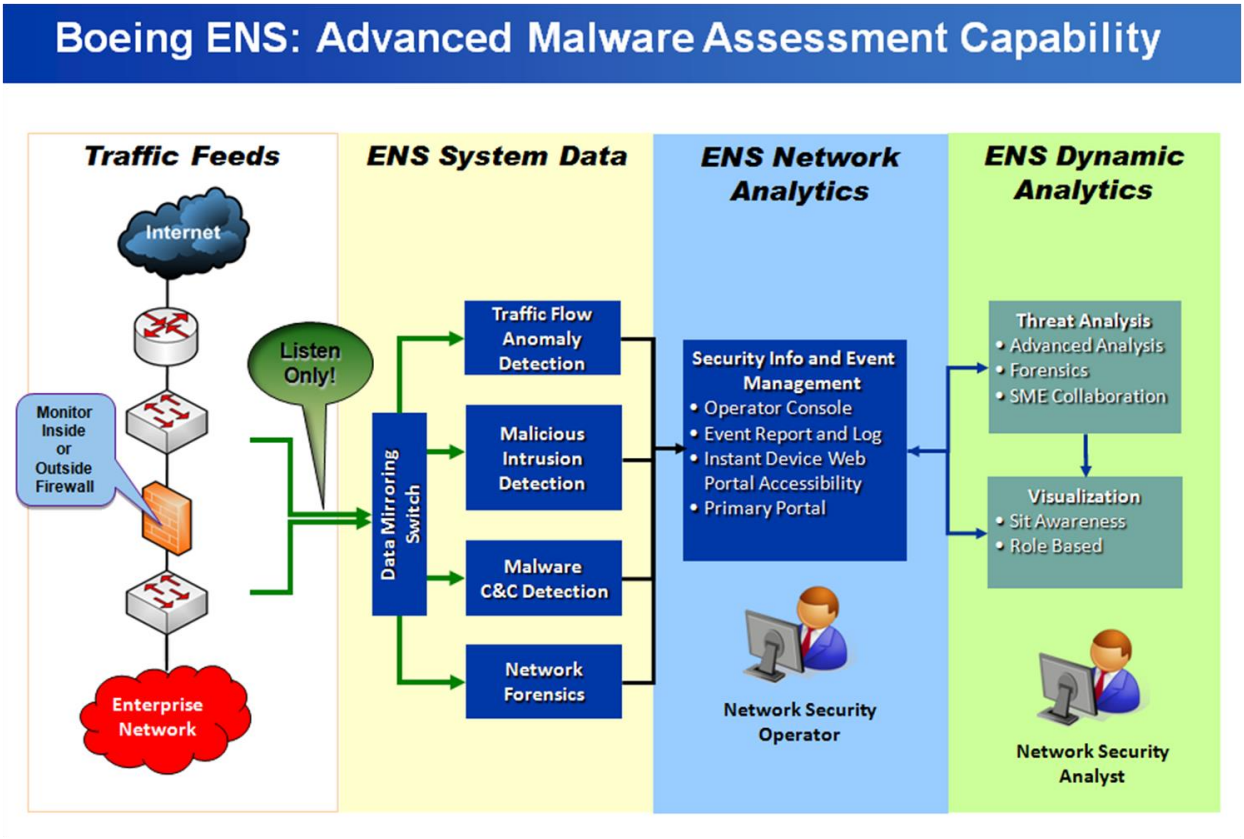
4.1 Enhanced SIEM - Path Forward

Continued development and deployment efforts will bring further system refinements through execution and evaluation of several Use Cases specifically developed for this implementation. Current uses cases cover a wide range of scenarios including: unauthorized Admin change detection, unauthorized communication detection, data exfiltration detection, and unauthorized configuration changes. Multiple iterations of this solution candidate are expected.

5. Enhanced Malware Assessment

Several deployments of Boeing's advanced malware assessment capability, called Enterprise Network Sentinel (ENS) have been performed on various PJM network systems. The ENS scanned PJM's enterprise, energy management, and SCADA network environments for advanced threats. The integrated, non-signature based approach to network anomaly and malware detection, includes the ability to perform real-time forensics, advanced correlation of security events, and response work flow management. Results from these deployments are being used to inform best actions toward maintaining the most robust defense possible against advanced zero-day and stealthy threats. Figure 4 illustrates an overview of the ENS capability used for these advanced malware assessments.

Figure 4- Advanced Malware Assessment Capability



5.1 Enhanced Malware Assessment - Path Forward

Current malware detection systems, while most effective against IP and E-mail protocols, lack the same level of robustness (or lack any capability at all) for SCADA system protocols. Continued development and deployment solutions activities are in work to extend the most advanced malware detection capabilities to SCADA system protocols such as DNP3 and ICCP.

6. Enhanced Application Security

Several iteration candidates are in progress that fall under the broad topic area of Application Security, completion of which is intended to establish a framework going forward to enhance overall effectiveness of the Application Security practices already in place at PJM.

Following the results of the Phase I Risk Based Assessment, Application Security improvement opportunities were identified for prioritization to focus efforts for maximal security posture benefit. Prioritization of development action plans for Application Security leaves open the opportunity to proactively posture for future Application Security issues.

To best address future Application Security issues, development of an Application Security Maturity Model specifically tailored for the unique requirements of electricity sector was initiated. Current electricity sector software is a mixed inventory of components acquired from external vendors and created by internal development teams. Additionally, software acquired from vendors may be customized internally for the organization's specific requirements. Given this mix, an appropriate maturity model must address both secure software development practices as well as secure software acquisition/procurement processes. This software mixture is typical of the vast majority of companies and organizations, therefore, the energy sector can benefit from the same maturity models and other tools that are available to those companies. However no single solution exists to meet the specific needs of the energy sector and multiple solutions create wasteful overlap and cumbersome implementation.

To address the unique needs of the energy sector, the application security team considered nine existing maturity models and rated each candidate against eleven factors, or evaluation criteria, that a maturity model for the energy sector must address. These evaluation factors were derived based on the team's collective experience in software development lifecycle, cyber security, and the requirements of energy sector organizations. Factors such as flexibility, tailor-ability, adaptability, and secure software development and procurement practices were used as the basis for evaluation. As a result, the application security team concluded that a hybrid Application Security Maturity Model derived from the Build Security In Maturity Model, version 4 (BSIMMv4) with augmentation and tailoring from three additional maturity models could form the basis of a robust Application Security model specifically targeted to the unique needs of the energy sector.

The resultant Application Security Maturity Model was tested and validated against PJM's needs and objectives through self-assessments and key personnel interviews.

6.1 Enhanced Application Security - Path Forward

With the determination of requirements, development, and validation of the Application Security Maturity Model complete, the project partners have developed a roadmap to take PJM's Application Security to the next level of sophistication. Next steps will focus on timelines and activities for formal rollout and implementation.

7. Summary

Guided by the results of the risk-based assessment completed in Phase I and detailed in TPR1, the Boeing-PJM team has begun multiple Phase II Development and Phase III Deployment activities designed to bring focused security solutions to PJM and create opportunities for replication in the energy sector.

The initial deployment of capabilities and technology integration has resulted in: 1) improvements to the Security Information and Event Management (SIEM) system resulting in better threat visibility, thus increasing the likelihood of detecting a serious event, 2)improvements in security posture visibility related to malware detection and zero-day threat response capability, and 3) development of an energy sector application security maturity model with associated assessment tool aimed at staying ahead of the threat posed by increasingly sophisticated cyber attacks.

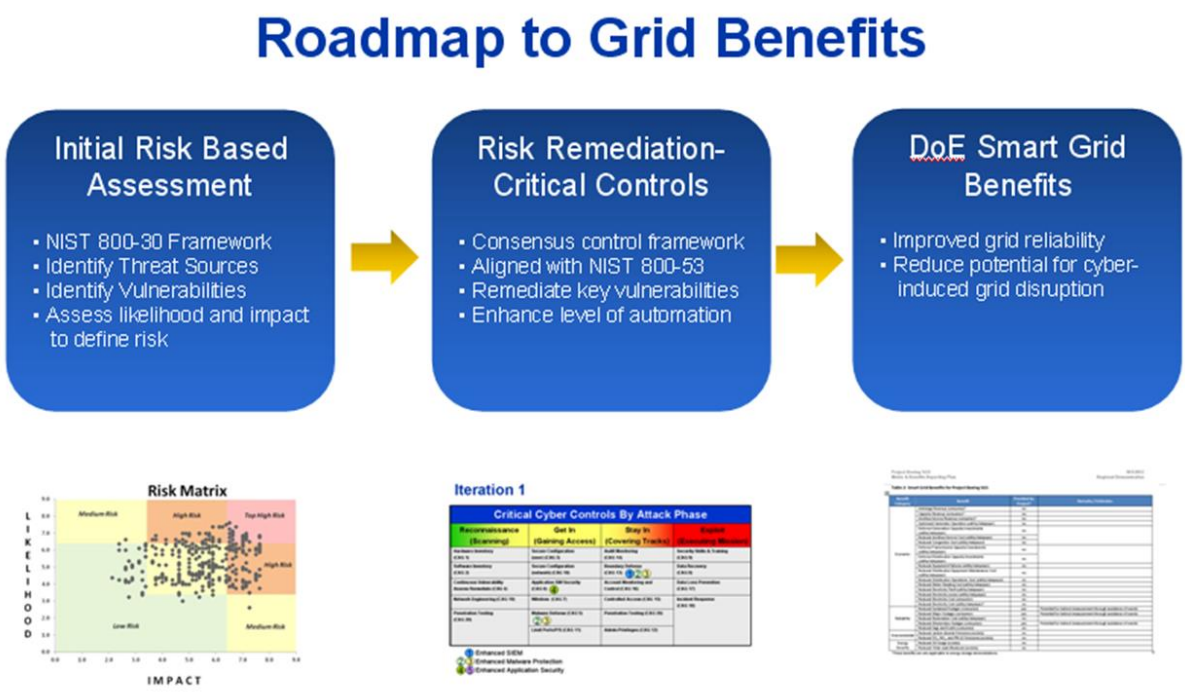
Solution development will continue in these areas and additional solution candidates are in work for future iterations. Subsequent Interim Technology Performance Reports will address the project team's ongoing development and deployment iterations and the remediation activities included in each. The 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- Roadmap to Grid Benefits

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 A1- Project Boeing SGS Linkage to Smart Grid Benefits



The key activities and outcomes of the Cyber-Security Risk Assessment are depicted graphically in the first block of Figure A1. 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 A1 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. As shown in Figure A2, 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.

Figure A2- 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-2.5 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.