Interim Technology Performance Report 3

PROJECT BOEING SGS

Contract ID: DE-OE0000191

Project Type: Regional Demonstration

Revision: V1

Company Name: The Boeing Company

November 19, 2013

TABLE OF CONTENTS

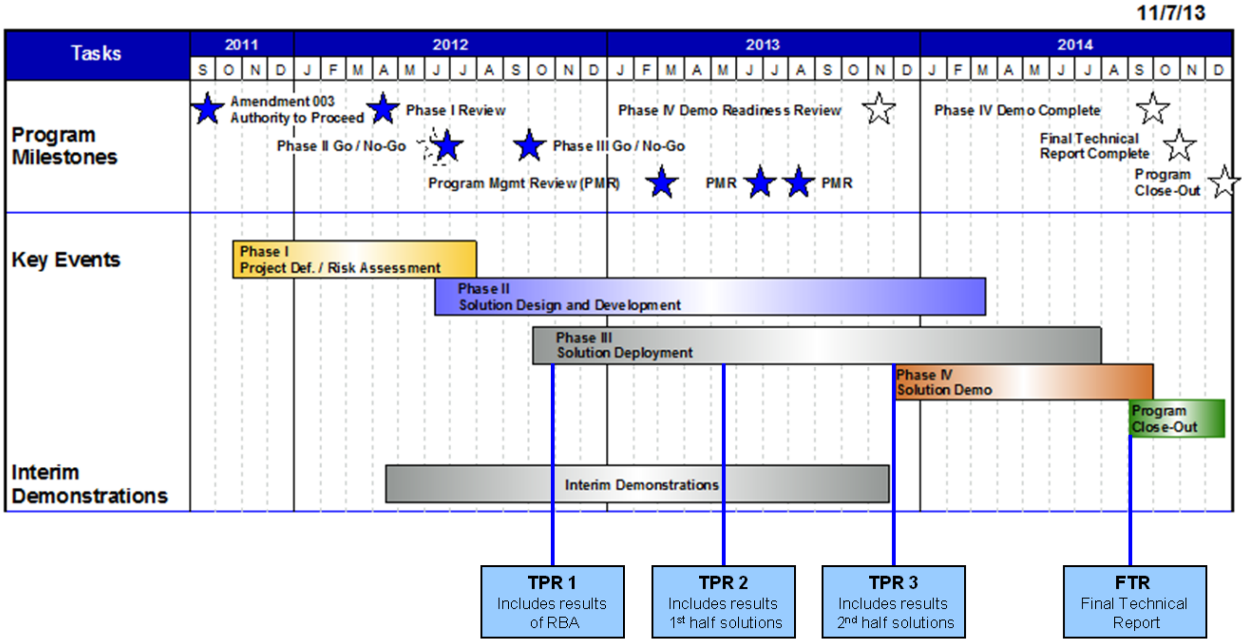
1. Contents

2. Introduction

This document represents the third 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 TPR3 on the Project Integrated Schedule shown in Figure 1, covers the later portions of Phase II Solution Design and Development and middle portion of the 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.

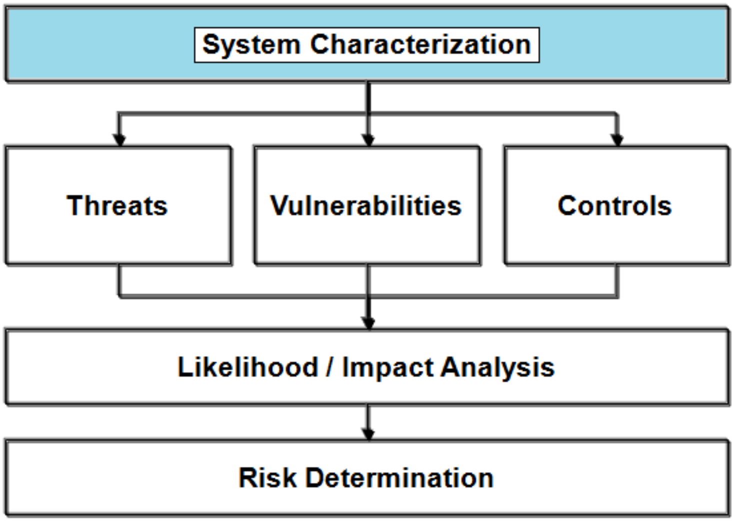
Figure 1- Project Boeing SGS Integrated Schedule



3. Risk Based Assessment / Solution Candidate Overview

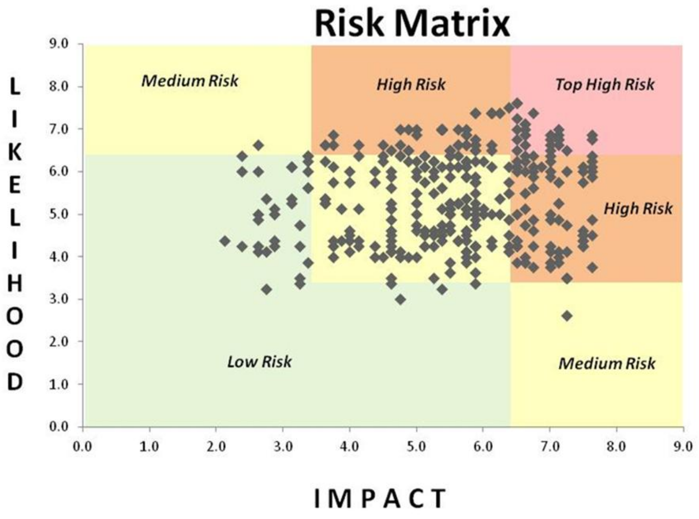
As detailed in TPR1, the Phase I Risk Based Assessment of PJM's high value information systems was undertaken and adhered to NIST Special Publication 800-30 (Risk Management Guide for Information Technology Systems) by executing the process while specifically tailoring step details for the energy sector.

Figure 2- Risk Assessment Process Overview



Mapping potential threat actors to potential vulnerabilities resulted in the risk matrix shown in Figure 3. 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- Threat – Vulnerability Risk Matrix



Guided by the risk assessment findings, the project team determined specific solution development activities likely to offer the greatest degree of security return relative to investment.

Prior solution candidates (covered in TPR-2) have included:

- Advanced Malware Detection
- Application Security
- SIEM Optimization

This report (TPR-3) covers:

- further enhancements to SIEM implementation
- Continuous Vulnerability Monitoring
- SCADA Monitoring and Intrusion Detection

4. Enhanced Security Incident and Event Management (SIEM)

The Security Incident and Event Management (SIEM) system continues to serve as the key integration platform in the development and deployment activities at PJM. Enhancements and optimizations to the SIEM that were introduced in TRP2 included the creation and integration of a threat dashboard, along with filtering and stratification of critical alerts into the appropriate phase of the Advanced Persistent Threat (APT) life cycle. The resulting system has matured through follow-on design and deployment iterations with the resulting system realizing a host of benefits:

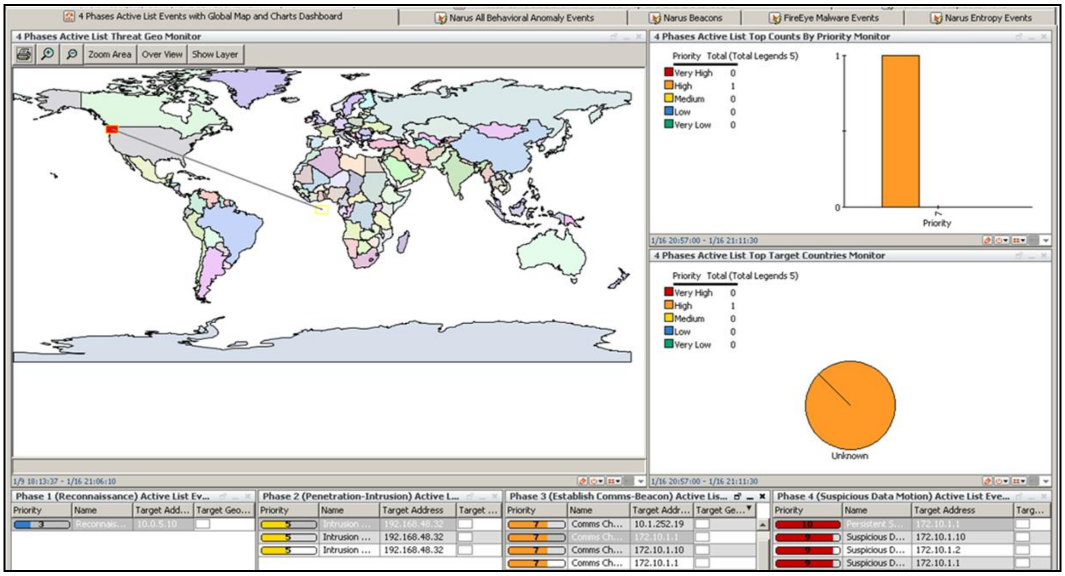
- improved operator efficiency due to a more manageable number of reported alerts
- better timeliness and precision due to reduction of noisy “false positive” alerts
- greatly enhanced situational awareness due to alert reporting within the APT threat life cycle

Achieving the above benefits required a full inventory of all potential monitoring devices and data connectors with special attention to ensuring error free parsing. As such, the SIEM has evolved into the primary cyber security situational awareness user console for information security monitoring. Figure 4 shows an example situational awareness dashboard with threat phase stratification of security alerts.

The focus of follow-on design and development iterations has been to advance the SIEMs functional role as the security situational awareness console through the integration of reporting events from a wider set of security tools into the SIEM dashboard. Specifically, the following capabilities have been integrated and deployed to demonstrate the potential of expanded monitoring capability:

- Integrated reporting of continuous vulnerability scans down to layer three devices. This is new capability as described in Section 5 of this document.
- Integrated reporting of dedicated SCADA Intrusion detection and monitoring system. This is new capability as described in Section 6 of this document.

Figure 4- Example SIEM Situational Awareness Dashboard


4 Phases Active List Events with Global Map and Charts Dashboard
Narus All Behavioral Anomaly Events
Narus Beacons
FireEye Malware Events
Narus Entropy Events
4 Phases Active List Threat Geo Monitor
Zoom Area
Over View
Show Layer
1/9 18:13:37 - 1/16 21:06:10
4 Phases Active List Top Counts By Priority Monitor
1
0
7
Priority
1/16 20:57:00 - 1/16 21:11:30
4 Phases Active List Top Target Countries Monitor
Unknown
1/16 20:57:00 - 1/16 21:11:30

Priority	Total (Total Legends 5)
🟥 Very High	0
🟧 High	1
🟨 Medium	0
🟦 Low	0
🟩 Very Low	0

Priority	Total (Total Legends 5)
🟥 Very High	0
🟧 High	1
🟨 Medium	0
🟦 Low	0
🟩 Very Low	0

Phase 1 (Reconnaissance) Active List Ev...

Priority	Name	Target Add...	Target Geo...
3	Reconnais...	10.0.5.10	□

Phase 2 (Penetration-Intrusion) Active L...

Priority	Name	Target Address	Target ...
5	Intrusion ...	192.168.48.32	□
5	Intrusion ...	192.168.48.32	□
5	Intrusion ...	192.168.48.32	□

Phase 3 (Establish Comms-Beacon) Active Lis...

Priority	Name	Target Addr...	Target Ge...
7	Comms Ch...	10.1.252.19	□
7	Comms Ch...	172.10.1.1	□
7	Comms Ch...	172.10.1.10	□
7	Comms Ch...	172.10.1.1	□

Phase 4 (Suspicious Data Motion) Active List Eve...

Priority	Name	Target Address	Targ...
10	Persistent S...	172.10.1.1	□
9	Suspicious D...	172.10.1.10	□
9	Suspicious D...	172.10.1.2	□
9	Suspicious D...	172.10.1.1	□

5. Continuous Vulnerability Monitoring and Management

Continuous Vulnerability Monitoring capability provides dynamic awareness of network vulnerabilities resulting from unforeseen network device configuration settings or inadvertent configuration changes that could pose a risk to a robust network security posture. Regular scanning prevents undesirable or unintended consequences resulting from architectural and operational changes by quickly detecting inadvertent or malicious system changes and enabling proactive response. This capability also facilitates effective patch management prioritization and verification.

The design, development and deployment of this capability at PJM consisted of designing the implementation architecture, deploying enhanced scanning tools, and then integrating new capability with legacy configuration management tools and scanners already in use by PJM.

Implementation at PJM resulted in successful demonstration of Layer 3 device scans capable of detecting network configuration changes in areas such as firewall settings, router or switch access control lists (ACLs), new device additions, as well as deviations from Best Practices.

The development effort also resulted in the integration of scan results to the SIEM dashboard for alert reporting to security operators, thus demonstrating the potential for enabling a greater level of situational awareness to security personnel and providing improved anomaly response time.

A few key “lessons learned” from the deployment are worth noting:

- Legacy devices may pose challenges to performing Layer 3 scans in a completely benign manner. If these devices are critical to the organization’s mission, then resource requirements to safely resolve these issues without negatively impacting operations may become significant.

- Determining optimal scanning frequency (daily, weekly, monthly) will likely be situation dependent based on the change dynamics and criticality of the subject network devices.

- Integrated vulnerability scans at the Layer 3 device level provide excellent network mapping and visualization capability which directly benefits overall network analysis capability.

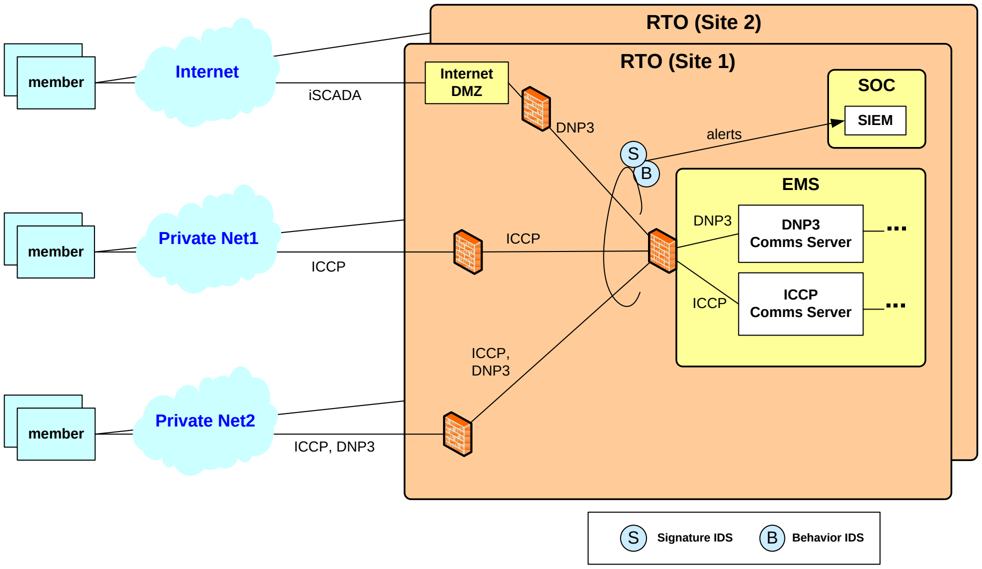
6. SCADA Monitoring and Intrusion Detection

SCADA network monitoring and intrusion detection has been identified as a high value technology in the electric sector, and in general, across much of the energy sector. The maturity and availability of TCP/IP intrusion detection systems (both behavioral and signature based) has advanced rapidly in recent years, but few options exist for robust protection of SCADA networks. The objective of this solution candidate was to develop, deploy, integrate, and test robust SCADA Monitoring and Intrusion Detection System (SCADA-IDS) in PJM's representative electric sector environment.

Given the wide range of protocols used in SCADA applications, the SCADA-IDS must support a multitude of common industrial control system protocols. ICCP and DNP3 protocol compatibility was specifically developed for this implementation. Other compatible protocols include: OPC-DA, Modbus/TCP, IEC 60870-5-101/104, IEC 61850, MMS, RPC/DCOM, SMB/CIFS, and HTTP.

As depicted in Figure 5, a representative architecture was developed to serve as a template for solution development. Intrusion detection sensors positioned post firewall feed the SCADA-IDS where traffic content is screened for anomalies using both signature-based and behavioral-based detection techniques. Alerts generated by the SCADA-IDS are prioritized and sent to the Security Information and Event Manager (SIEM) and presented to security operator for disposition.

Figure 5- SCADA Network and Monitoring Architecture



Given the general availability and maturity of signature based detection capability and the limited effectiveness of signature based defenses to zero day attacks, project requirements skewed largely toward implementing and testing complimentary behavioral-based anomaly detection.

The behavioral detection engine evaluates communication patterns, protocol specifics, message types, message fields, message values, and other parameters to detect anomalous activity patterns and then provides detailed alerts to systems security operators for in depth analysis and timely response. The technology is self learning and can adapt to the complete range of legitimate network activity while detecting and alerting to real anomalies posed by advanced cyber attacks, human errors, or poor network configurations.

The SCADA-IDS has undergone testing in the PJM environment in order to refine operational configurations and end use system requirements. Given the need to test the SCADA-IDS against live threats without introducing risk to the PJM test environment, additional test facilities were required. To enable advanced testing and to further develop SCADA threat detection capability, Boeing has developed a SCADA test bed where known SCADA exploits can be injected and evaluated in a controlled environment. New test cases can also be developed in this facility to identity and study heretofore unexploited SCADA vulnerabilities and develop remediation steps to prevent future risk of exploitation.

7. Summary

Guided by the results of the risk-based assessment completed in Phase I and detailed in TPR1, the Boeing-PJM team has completed multiple iterations through the Phase II Development and Phase III Deployment phases. Cyber security solution efforts in Application Security, Enhanced Malware Detection for enterprise networks, and SIEM Optimization were reported in TPR-2. Follow-on efforts in SIEM Optimization, and additional solution development in Continuous Vulnerability Monitoring, and SCADA Monitoring / Intrusion Detection were described in this third Technology Performance Report. All development and deployment solutions are intended to be applicable for demonstration at PJM and suitable for replication across the energy sector.

Benefits identified to date include:

- Improved Security Information and Event Management (SIEM) system resulting in better threat visibility, thus increasing the likelihood of detecting a serious event
- Improved malware detection and zero-day threat response capability
- Improved ability to systematically evaluate and secure in house and vendor sourced software applications

- Improved ability to continuously monitor and maintain secure configuration of network devices resulting in reduced vulnerabilities for potential exploitation
- Improved malware and intrusion detection capability on critical SCADA networks including behavioral-based alerts resulting in improved zero-day threat protection
- Improved overall cyber security situational awareness through the integration of multiple discrete security technologies into a single cyber security reporting console

Solution design, development, and deployment will continue into 2014 to further mature solutions and explore new technologies to enhance network security incident response and recovery. In addition, Phase IV Demonstration efforts will begin in parallel to showcase project insights and findings to date.

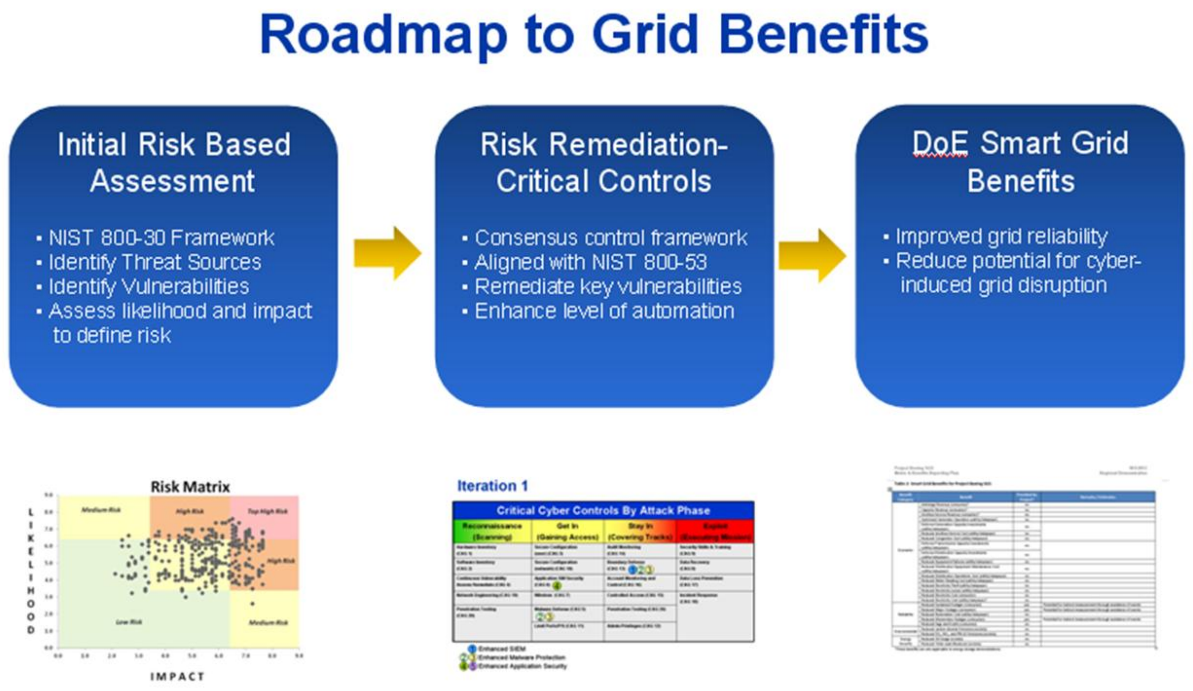
The next planned project report will be the Final Technical Report which will be a comprehensive document including all TPR content to date, any remaining solution accomplishments, and a reassessment of the cyber security risk matrix to evaluate overall cyber security risk reduction accomplished through 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



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

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.