| | |
|---|---|
| **Association of Home Appliance Manufacturers (AHAM) Smart Grid Task Force** | • Whirlpool is a board member of the Association of Home Appliance Manufacturers, and helps lead the effort for a common standard and object model for Smart appliance communication. Whirlpool also promotes and encourages the adoption of common standards for the appliance industry.<br>• Whirlpool actively monitors development of the following emerging standards: ANSI/AHAM CHA-1-2003 - Connected Home Appliances - Object Modeling |

## 3.2 CYBER SECURITY SUMMARY

Cyber security is a critical element in the development and deployment of a viable Smart Grid. Whirlpool's proposed architecture employs proven security technology in a multi-tiered approach to secure each step in the communication and control process: from the home area network, across the Internet Domain and Smart Meter Domain, to the Smart Grid Control. These open security frameworks and protocols encrypt and transport data and messages while protecting connections from tampering, theft, and malicious activity. Additionally, this security framework allows configuration of various security levels for different areas of the network, different applications, and different nature of data, on a real-time basis. Since these technologies are already proven in the public sphere, they provide unbreakable security today, and the flexibility to adapt to emerging threats in the future.

### 3.2.1 WHIRLPOOL'S CYBER SECURITY ARCHITECTURE

(b)(4)

(b)(4)

### 3.2.2 CYBER SECURITY RISKS AND MITIGATION

Whirlpool's multi-level security measures cover a wide array of identifiable and potential security vulnerabilities. Our security mitigation solution not only protects assets in the proposed Whirlpool's architecture, but will also help to protect the Smart grid itself. A summary of the different cyber security risks and the associated mitigation plans are described in Table 8.

**TABLE 8 – SUMMARY OF CYBER SECURITY RISKS AND MITIGATION PLAN**

| Scenario Description (Threat/Vulnerability) | Impact to the System | Mitigation Plan |
|---|---|---|

(b)(4)

[redacted]

(b)(4)

[redacted]

(b)(4)

[redacted]

### 3.2.3 ADDRESSING SECURITY IN EVERY PHASE OF THE PROJECT

Security has been an integral focus of Whirlpool's design architecture since the program's inception. Following numerous NIST security guidelines, Whirlpool focused on ensuring data integrity since the Smart grid is an information system and providing incorrect or unreliable information is unacceptable. First, detailed security requirements were defined, along with technical and managerial solutions to potential risks. From these, a security plan was created.

Next, several review processes were performed with security professionals offering different perspectives to identify all potential risks and associated mitigations. This process also ensured that the Whirlpool's solution is realistic and cost-effective.

This process resulted in detailed security architecture, and uncovered numerous new requirements, such as the need for a random cryptographic number generator in the hardware manufacturing process, and redundant confirmation of demand response commands from the IP and AMI networks.

### 3.2.4 CRITERIA USED FOR VENDOR AND DEVICE SELECTION

A summary of criterions used by Whirlpool for evaluating vendors and devices is shown in Table 9.

**TABLE 9 – SUMMARY OF CRITERION FOR VENDOR AND DEVICE SELECTION**

| Criteria Description | Whirlpool's expectation |
|---|---|
| Size and Experience | Vendors should be established players with a proven track record of delivering results. |

| | |
|---|---|
| Technical | Vendor's solution to the technical issue should have a sound architecture. Vendors should also provide detailed test plans for their components, such as stability, load/stress, performance, redundancy, and other tests. |
| Service and Support | Vendor should be able to provide high-quality of service through the product life-cycle. |
| NIST standards | Vendors should meet Whirlpool's rigid quality standards on three different NIST metrics - trustworthiness, predictable execution, and conformance |

Additionally, Whirlpool evaluates, prepares and selects at least two third-party vendors for each component in the technical solution. This is done in a cost-effective manner so that if one vendor fails to deliver a component with satisfactory quality or quantity, a backup vendor can quickly take over.

### 3.2.5 SUPPORT FOR EMERGING SMART GRID CYBER SECURITY STANDARDS

Whirlpool's proposed architecture employs an array of open security standards and encryption techniques enabling the system to be easily customized and adapt to emerging security standards. The security architecture was developed according to numerous standards, the majority from NIST Special Publication 800 series, including NIST SP800-30, SP800-39, SP800-60, and SP800-64. Federal Information Processing Standards Publication by NIST also provides high level guidelines, including FIPS-200, FIPS-199, and FIPS-186-3. Whirlpool will also continue to work on Smart grid security standards with other organizations, including NERC, AMI-SEC, OpenHAN, and IEC, and is willing to open the design of security system to the wider community, such as a standards framework organized by NIST.

The most important document that informed our approach was "Report to NIST on the Smart grid Interoperability Standards Roadmap". Table 10 summarizes the standards that we plan to follow.

**TABLE 10 – SUMMARY OF SECURITY STANDARDS USED**

| Publication | Title |
|---|---|
| NIST SP800-30 | Risk Management Guide for Information Technology Systems |
| NIST SP800-39 | Managing Risk from Information Systems An Organizational Perspective |
| NIST SP 800-60 Rev.1 | Guide for Mapping Types of Information and Systems to Security Categories |
| NIST SP 800-64 Rev.2 | Security Considerations in the System Development Life Cycle |
| FIPS PUB 200 | Minimum Security Requirements for Federal Information and Information Systems |
| FIPS PUB 199 | Standards for Security Categorization of Federal Information and Information Systems |
| FIPS-186-3 | Digital Signature Standard (DSS) |
| NIST SP 800-82 | DRAFT Guide to Industrial Control Systems (ICS) Security |
| NIST SP 800-53 Rev. 3 | Recommended Security Controls for Federal Information Systems and Organizations |
| NIST SP 800-90 | Recommendation for Random Number Generation Using Deterministic Random Bit Generators |
| NIST SP 800-92 | Guide to Computer Security Log Management |
| NERC CIP 002-009 | A series of standards are directly relevant to the bulk power system critical cyber assets from NERC |
| IEC 61970 | The application program interfaces for energy management systems (EMS). |