The GridWise Alliance
Advocating for a Smarter Grid

September 2011

GridWise Alliance Principles for Grid Cybersecurity

The electricity industry is essential to all sectors of our nation's economic life, more so now than ever before. Preserving the mission of the grid, which is delivering safe, reliable electrical energy at an economically-viable cost, is the primary task of all operators and service providers. From smart meters to smart appliances to more intelligent control of distribution, transmission, and generation, an advanced grid offers the potential of improved utilization of all generation and storage resources, increased operational efficiency and reliability, and enhanced opportunity for customers to make choices about energy use. A more interconnected, automated, and information-rich electricity delivery system also provides the opportunity to deliver a safer and more reliable interoperation, and to mitigate threats to the grid and electric user's privacy from accidental and intentional harm. To be effective those responsible for securing the grid must be empowered to implement and manage these cybersecurity solutions within the enterprise. The GridWise Alliance believes that with sound planning, thorough design, and coordinated execution, a safe, secure, and reliable smart grid can be achieved. Interoperability and cybersecurity policies and legislation, and the resulting guidelines and standards will play a critical role in realizing a transformed electric grid. Outlined below are the key principles endorsed by the Alliance for cybersecurity.

1) **Involve All Stakeholders, Take Full Advantage of and be Aligned with Existing Recognized Processes and Work.**
   a. **Description:** The existing NIST-coordinated Cybersecurity Working Group process along with standards development underway at various standards organizations are an appropriate means to achieve the necessary framework of guidance for a secure smart grid. This work began with an effective call-to-action for stakeholders that were widely embraced by the industry. Additionally, the work being done at the North American Electric Reliability Corporation (NERC) and within such collaborations as the Department of Energy's Roadmap to Secure Energy Delivery Systems, the National Electric Sector Cybersecurity Organization (NESCO), and the Department of Homeland Security's (DHS) Industrial Control System Joint Working Group (ICSJWG) add to the body of available best practices. Supporting, extending and harmonizing this on-going work is key to completing the required framework on which a growing and evolving grid can be secured.

   b. **Benefit:** Maintaining momentum and minimizing redundant efforts provides the shortest and clearest path to a secure grid. In contrast, establishing new processes outside of the existing framework could result in competition with existing processes for resources; an increased number of gaps and conflicts; confusion regarding the direction and specifics of requirements; and possible result in less timely, less robust outcomes. Embarking on one or multiple separate efforts will further strain the limited resources available to reach consensus and develop an effective framework.

   c. **Example:** The emerging work between UCA and ASAP-SG to ensure alignment of these group activities with overall NIST-SGIP efforts

   d. **Implications**: Enhanced education and alignment across the grid's stakeholders, thereby improving the security posture of the electric system. Because the systems are interconnected both technically and from the perspective of the customers, every participant has a responsibility to follow the guidance.

2) **Utilize a Comprehensive Risk Management Approach.**

   a. **Description**: All smart grid projects must consider a risk-based approach to selecting and implementing security controls that provide operationally effective and cost-effective security commensurate with potential impacts to safe and reliable power delivery. The value or criticality of each threat must be assessed in contrast to the potential risk to safe and effective energy delivery. This risk management approach should incorporate a quantifiable value at risk (e.g. dollar) including the determination of how likely a risk is to occur and the potential loss associated with that risk. If a quantifiable value of risk is impractical to be determined, then a qualitative value of risk analysis should be preformed following an accepted methodology.

   b. **Benefit**: Consistent approach to risk assessment with subsequent valuation in monitoring security as applied to each case. Ability to learn and evolve threat assessment practices. Practical application of secure technology and practices based on the value of specific threats.

   c. **Example**: Risk Management Guide for Information Technology Systems, NIST Special Publication: 800-30; Guide to Industrial Control Systems Security, NIST Special Publication 800-82

   d. **Implications:** The determination of threats, vulnerabilities and their impacts based on an overall risk management approach allows resources to be deployed where they provide the most benefit to grid security.

3) **Provide Clarity to All Stakeholders.**

   a. **Description**: Guidance, regulations and standards addressing cybersecurity must be understood by all parties and implemented by a wide range of utility asset owners, operators, vendors, and service providers. Clarity is mandatory to enable all stakeholder groups to effectively use developed guidance, standards and regulations. As in the general NIST guidelines – NISTIR 7628 -- the roles and responsibilities of each stakeholder must be clearly articulated. Standards should enable a stakeholder to meet established business requirements or use cases without specifying how that requirement or use case should be accomplished by the party.

   b. **Benefit**: Asset owners, operators, and service providers will be able to understand the objectives and requirements of guidance, regulations and standards. Minimal time will be wasted on interpretation by either utilities or regulators; emphasis will be on implementation and compliance to achieve security. Vendors will be able to focus R&D efforts on smart grid components that not only enhance security but also meet compliance requirements.

   c. **Example**: ISO/IEC 27032, FIPS 140-2 and the associated cryptographic module and algorithm validation programs

   d. **Implications:** Smart Grid components, systems, and projects will be able to move quickly to secure status, with certifiable or at least verifiable capabilities.

4) **Construct Cybersecurity Framework that is Focused Specifically for Electric Grid Applications.**
    a. **Description**: Cybersecurity for all national critical infrastructure and industries is an important principle of national security. Within that broad framework, grid cybersecurity has specific characteristics and requirements that must be addressed. Grid domain requirements make it imperative that policy and standards be developed specifically to meet those needs. Direct application of cyber security requirements, standards, regulations, and solutions outside our domain may not result in material improvements to grid cybersecurity and possibly raise costs and/or hinder operational effectiveness.

    b. **Benefit**: Policy and standards can be developed more quickly, with less intra-agency communication and overhead. Cybersecurity for the grid can be implemented and verified without the burden of non-domain requirements that would add little or no value to its overall system effectiveness and resilience.

    c. **Example**: NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security , NISTIR 7628, Guidelines for Smart Grid Cybersecurity

    d. **Implications:** Cybersecurity policies, practices, standards, and solutions optimized to meet the needs of the grid rather than another domain or discipline.

5) **Create and Adopt Uniform Verification and Test Procedures for Standards and Guidelines.**
    a. **Description**: To be effective, any standard associated with cybersecurity must be verifiable and testable thus providing asset owners and service providers with firm targets and known processes and procedures for testing and verification which is crucial for achieving cybersecurity objectives. Assigning the responsibility for security testing and verification is equally important to effective adoption and true cybersecurity. It is important that those testing smart grid components and systems have easy to follow guidelines and procedures that will help them verify the component or systems has been sufficiently secured.

    b. **Benefit**: Clear direction and methods for asset owners, service providers, and vendors to enable investment in appropriate technologies and work processes for securing the smart grid. Well-established process responsibility for security testing and verification will facilitate corrective action to improve grid security.

    c. **Example**: ISO i5408, Common Criteria; Zigbee compliance “plug fest”; DOE LEMNOS, STIG Security Technical Implementation Guide - DISA

    d. **Implications:** Confidence in deployed solutions.