White Paper for NIST CSWG: AMI System Security Requirements, Organized by Interface Category

(Extracts from an EPRI-sponsored project developed by Frances Cleveland, Xanthus Consulting International)

Table of Contents

1. Introduction

1.1 Cyber Security: Balancing Costs versus Impacts

Cyber security must balance the cost of implementing security measures against the likelihood and impact of any security breaches. This balancing of cost vs. impact must take into account that excessive costs could impact customer rates, but that inadequate security measures could allow unnecessary power outages to those same customers. The cost/impact balancing also must recognize that no single security measure is 100% effective in preventing a security breach. Therefore, layered security measures must be applied, and methods must be developed for deterring, detecting, and coping with security attacks, along with audit trails for forensic analysis, possible legal actions, and training.

The first step in determining a good cost/impact balance is to develop security requirements for all "cyber assets", where these assets can be defined as physical systems/equipment, stored cyber software and information, and information flows between systems. *The latter assets, "the information flows between systems" can be considered the critical assets for determining the cyber security requirements and ultimately the cyber security solutions.*

1.2 Cyber Security: Implementation Driven

Cyber security solutions must ultimately be implementation-specific, driven by the requirements for security of all of the functions in the system. However, "typical" security requirements can be developed and used as checklists for actual implementations.

In corporate settings, security requirements address the confidentiality, integrity, and availability of data using "Information Technology (IT)" security solutions such as cryptography, certificates, and physical access control. However, in the Smart Grid, the complexity of stakeholders, systems, devices, networks, and environments precludes just IT security techniques or one-size-fits-all security solutions. Therefore, additional criteria must be used in selecting the cyber security measures. These additional criteria must take into account the constraints posed by device and network technologies, legacy systems, organizational structures, regulatory and legal policies, and cost criteria. They should also take advantage of the existence of sophisticated equipment and systems that are already being used in the power system industry.

1.3 Cyber Security: Utilization of Existing Power System Management Capabilities

Power system operations have been managing the reliability of the power grid for decades in which "Availability of Power" has been a major requirement, with the "Integrity of Information" as a secondary but increasingly critical, requirement. "Confidentiality of Customer Information" has also been vitally important in the normal revenue billing processes. Although focused on inadvertent security problems, such as equipment failures, careless employees, and natural disasters, many of the methods, technologies, and mindsets can be expanded to cover deliberate security attacks as well.

So, one of the most powerful security solutions is to utilize and expand existing power system management technologies to provide additional security measures. After all, these power system management technologies (e.g. SCADA systems, Energy Management Systems, Contingency Analysis applications, Fault Location, Isolation, and Restoration functions, as well as Revenue Protection capabilities) have been refined for years to cope with the ever-increasing reliability requirements and complexity of power system operations, and are designed to detect anomalous events, notify the appropriate personnel or systems, cope during a problem, take remedial actions, and log all events with very accurate timestamps.

In the past, there has been little need for distribution management except possibly some load shedding to avoid serious problems. In the future, with generation, storage, and load on the distribution grid, utilities will need to implement more sophisticated power-flow-based applications to "manage" the distribution grid. AMI systems can also be used to provide energy-related information and act as secondary sources of information These same capabilities could be designed to help manage security as well.

Metering has also addressed concerns about revenue protection and customer confidentiality for many years, although the advent of smart meters has expanded those concerns to a significant degree. However, many of the same concepts of revenue protection could also be used for the smart grid.

In fact, expanding existing power system management capabilities to cover specific security requirements, such as power system reliability, should be a major security requirement.

2. Key Security Controls Derived from the DHS Catalog

The DHS "*Catalog of Control Systems Security*" covers most areas of concern for power-related management systems, although some many need interpretation or expansion as to how they apply to the different interfaces. In particular, many of these systems have the capability of monitoring and analyzing significant amounts of information from the field. Some of this information, whether raw or analyzed, could be used to detect security anomalies, take preventative or coping actions, and provide audit trails for subsequent security analysis. Therefore, these monitoring and analysis capabilities should be utilized as part of the security measures for mitigating security "attacks", whether deliberate or inadvertent.

The following sections cover at a high level some of the key security requirements of particular applicability to AMI systems, power system operations, and HAN systems, or of particular concern where special security issues need be identified. *(Section 3 addresses AMI system security requirements in more detail.)*

Subsections in italics are not in the DHS document, but reflect certain specific security control requirements or caveats for power related systems, such as:

– *AMI systems, including their interfaces to back office systems as well as to the meter and customer sites. AMI systems can provide monitoring and control as well as analysis of anomalous situations.*

- *Power system operational systems (e.g. SCADA/EMS/DMS) which interface with field equipment. These real-time systems can monitor and control field equipment, and can use power-flow-based algorithms to assess power system situations.*
- *Inter-field equipment interfaces with other field equipment, whether within a substation, on transmission lines, or on distribution feeders. Intelligent field equipment can monitor and control themselves and sometimes other field equipment, and provide some basic analysis capabilities.*
- *Engineering systems which can interface with field equipment in non-real-time for establishing settings, issuing updates, running diagnostics, providing maintenance, etc.*
- *Home Area Network (HAN) or Building Area Network (BAN) or Neighborhood Area Network (NAN) systems which involve energy-related interactions, such as demand response (DR), management of distributed energy resources (DER), energy usage monitoring, plug-in electric vehicle (PEV) charging management, etc. The HAN interfaces include those within the customer site as well as between the customer site and external parties such as to the utility via the AMI system or to aggregators via public or private networks.*

Systems on HANs present particular challenges since there is no single authority to manage the combination other than the customer, who generally is not a security expert. Therefore, security on HAN systems will entail product-by-product security, with HAN standards and recommended practices used to enforce the security requirements.

Unless specifically indicated separately, these systems will be referred to generically as Power-Related Management (PRM) systems.

2.1 Security Policy

The organization develops, implements, and periodically reviews and updates:

1. A formal, documented, control system security policy that addresses:
   a. The purpose of the security program as it relates to protecting the organization's personnel and assets;
   b. The scope of the security program as it applies to all the organizational staff and third party contractors;
   c. The roles, responsibilities, and management accountability structure of the security program to ensure compliance with the organization's security policy and other regulatory commitments.
2. Formal, documented procedures to implement the security policy and associated requirements. A control system security policy considers controls from each of the families contained in this document.

- *All Power-Related Management (PRM) systems should have specific security policies not only for personnel, but for the management of the systems, software applications, field equipment, and interfaces.*

2.2 Organizational Security

Organizational security involves setting organization-wide policies and procedures that define acceptable behavior and practices concerning security. Organizational security includes management accountability, physical controls, and cyber – related functions. Organizational policies and procedures specify direction, commitment, responsibility, and oversight and define the security posture for the control system. These policies and procedures also apply to third-party contractors, integrators, and vendors utilized by the organization.

- **Management Policy, Procedures, and Accountability**: The organization establishes policies and procedures to define roles, responsibilities, behaviors, and practices for the implementation of an overall security program. The organization also defines a framework of management leadership accountability. This framework establishes roles and responsibilities to approve cyber security policy, assign security roles, and coordinate the implementation of cyber security across the organization.
  - *PRM systems monitor and analyze significant amounts of information from the field. Some of this information, whether raw or analyzed, could be used to detect security anomalies. Therefore, these monitoring and analysis functions should be utilized as part of the security measures for preventing, detecting, and/or deterring any security "attack", whether deliberate or inadvertent. All potential security violations should be monitored, and appropriate security personnel and/or systems notified.*
  - *IEC 62351 Part 8 on Role-Based Access Control (RBAC) will provide methods for handling personnel and software application roles and responsibilities for interactions involving the Common Information Model and/or IEC 61850 implementations. The same RBAC capabilities should also be used for all other interactions.*
- **Coordination of Threat Mitigation**: The organization's security policies and procedures delineate how the organization implements its emergency response plan and coordinates efforts with law enforcement agencies, regulators, Internet service providers and other relevant organizations in the event of a security incident.
  - *PRM systems should be used as part of the threat mitigation policies by using their inherent monitoring, control, and analysis capabilities to detect, defer, and provide audit trails for the organizations in the event of a security incident..*
  - *Power system operational requirements should play a key role in this coordinated response, including the use of power flow-based contingency analysis and other available operations emergency response capabilities.*
  - *Depending upon where and how a security incident affects power system operations, the AMI systems may be able to provide additional information, either to corroborate or substitute real-time monitoring data or to identify the impact of the security incident more precisely.*
- **Security Policies for Third Parties**: The organization holds external suppliers and contractors that have an impact on the security of the control center to the same security

policies and procedures as the organization's own personnel. Ensure security policies and procedures of second- and third-tier suppliers comply with corporate cyber security policies and procedures if they will impact control system security.

- *Contractors providing meters and other sensitive AMI equipment should have a secure process in place for "rolling over and updating" factory-provided security certificates and keys to the owner of the equipment to ensure no tampering or unauthorized access to this sensitive equipment can occur.*

2.3 Personnel Security

Personnel security addresses security program roles and responsibilities implemented during all phases of staff employment, including staff recruitment and termination. The organization screens applicants for critical positions in the operation and maintenance of the control system. The organization trains personnel when they are hired and provides subsequent refresher training on their job tasks, responsibilities, and behavioral expectations concerning the security of the control system. The organization may consider implementing a confidentiality or nondisclosure agreement that employees and third-party users of control system facilities must sign before being granted access to the control system. The organization also documents and implements a process to secure resources and revoke access privileges when personnel terminate.

- **Personnel Security Policy and Procedures**: The roles, responsibilities, and management accountability structure of the security program to ensure compliance with the organization's security policy and other regulatory commitments; to review and document list of approved personnel with access to control systems.
  - *IEC 62351 Part 8 on Role-Based Access Control (RBAC) will provide methods for handling personnel and software application roles and responsibilities for interactions involving the Common Information Model and/or IEC 61850 implementations. The same RBAC capabilities should also be used for all other interactions.*

2.4 Physical and Environmental Security

Physical and environmental security encompasses protection of physical assets from damage, misuse, or theft. Physical security addresses the physical security mechanisms used to create secure areas around hardware. Physical access control, physical boundaries, and surveillance are examples of security practices used to ensure only authorized personnel are allowed to access control system equipment. Environmental security addresses the safety of assets from damage from environmental concerns.

- **Physical access authorization, control, and monitoring**: The organization develops and maintains lists of personnel with authorized access to facilities containing control systems and issue appropriate authorization credentials (e.g., badges, identification cards, smart cards). The organization utilizes physical access devices (e.g., keys, locks, combinations, card readers) and/or guards to control entry to control system facilities and assets. The organization monitors physical access to the control system facilities to detect and respond to physical security incidents.

  - *For AMI systems, the AMI Headend should be in physically protected facilities. However most AMI equipment is in field or customer locations that are impractical or impossible to completely protect physically. For this equipment, the primary requirement is monitoring and alarming on any unauthorized physical access attempts, physical disconnects from communications, and removal from the site.* ***This physical security monitoring should be added to any AMI system deployment.***
  - *For power system real-time operations and engineering management operations,* ***all field equipment, whether within substations or on pole-tops or other field locations, should add physical security monitoring to normal SCADA monitoring of power system information.*** *This physical security monitoring should cover locks, gates, doors, cabinets, enclosures, power sources, equipment on-off status, etc. All authorized physical access to this field equipment should identify the individual and the role of the individual.*
  - *For HAN, BAN, and NAN systems,* ***all sensitive equipment should have their physical security monitored.***

- **Delivery and removal**: The organization authorizes and limits the delivery and removal of control system components (i.e., hardware, firmware, software) from control system facilities and maintains appropriate records and control of that equipment. The organization documents policies and procedures governing the delivery and removal of control system assets in the control system security plan.
  - *For PRM systems, the hand-over from vendor to owner of sensitive equipment must ensure that the equipment's integrity and certification is not compromised. This includes the "roll-over" of security certificates or keys during the hand-over.*
- **Physical device access control**: The organization employs hardware (cages, locks, cases, etc.) to detect and deter unauthorized physical access to control system devices.
  - *For PRM systems, physical device access control must extend to the detection of theft, disconnection from communications, and disconnection from power.*

2.5 System and Services Acquisition

Systems and services acquisition covers the contracting and acquiring of control system components, software, and services from third parties.

- **Acquisitions**: The organization includes security requirements and/or security specifications, either explicitly or by reference, in control system acquisition contracts based on an assessment of risk.
  - *For PRM systems, all specifications for purchasing equipment should include security requirements not only for operating the fully installed equipment, but also for factory security, transport to the field site, transfer of security responsibility to the new owner, upgrade and patching security, maintenance security, moves and changes security, and replacement security.*

- **User-installed or out-sourced software**: The organization implements policies and procedures to enforce explicit rules and management expectations governing user installation of software.
  - *For AMI systems, almost all AMI Headend systems are customized to accommodate interfaces to different back office systems. Whether these customizations are contracted out to the AMI vendor, out-sourced to a third party, or performed in-house, the customized software must abide by the same security requirements as the base system, including all interfacing rules, testing, upgrade management, patch management, certificate management, etc.*
  - *For interfacing to legacy systems that cannot (practically) abide by these security requirements, alternate methods must be put in place to handle these situations, including additional monitoring of those interfaces, tighter restrictions on methods or types of data that can be exchanged (e.g. one-way only or aggregated data only), extensive logging of all alarms and events, etc.*
  - *For HAN/BAN/NAN systems, the policies and procedures will be more difficult to enforce since the equipment and software will be handled by the customer. Therefore, the interfaces between customer software and utility systems must have very strong rules and restrictions built in.*
- **Vendor Configuration Management, Security Testing, and Life-Cycle Practices**: The control system vendor creates and implements a configuration management plan and procedures that limit changes to the control system during design and installation. The vendor also plans and executes security testing, and develops life-cycle practices.
  - *In particular, meters must be certified as revenue grade and must remain securely certified between factory floor, shipment, warehousing, and installation. Vendors must not only ensure this revenue-grade security while under their control, but during any meter patches and upgrades.*
  - *Upgrades and patch management for any PRM sensitive equipment must include extensive re-testing to ensure the patches have not introduced any security holes or compromised certification. Vendors must be required to provide this re-testing and/or re-certification.*

2.6 Configuration Management

Control systems need to be configured properly to maintain optimal operation. *Vendors must initially design and configure these control systems properly with respect to security rather than adding security later.*

Therefore, only tested and approved changes should be allowed on a control system. Vendor updates and patches need to be thoroughly tested on a non-production control system setup before being introduced into the production environment to ensure no adverse effects occur.

- **Configuration change monitoring and control**: The organization authorizes, documents, and manages changes to the control system. The organization implements a process to monitor changes to the control system and conducts security impact analyses to determine the effects of the changes. Configuration change control involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the control system, including upgrades and modifications.

  - *AMI systems will change configurations frequently as meters are deployed and additional equipment is added. Although some of these changes are just system extensions, some may involve changes in equipment, changes in information flows, and changes in security management. For instance, key communication nodes may need to be "re-booted" to force a re-configuration to handle new dynamics.*
  - *Some configuration changes may be "dynamic", for instance, for establishing alternate communication paths when the primary path fails. Security controls must be designed and tested for expected dynamic changes.*
  - *The AMI system itself should be used to monitor and log these configuration changes, with notifications to security personnel if the configuration changes are not authorized or warranted by normal circumstances.*
  - *SCADA and network management systems used in power system operations should also be used to monitor and log configuration changes to networks used in these systems.*

- **Configuration settings**: Establishes mandatory configuration settings for IT products employed within the control system. Configures the security settings of control systems technology products to the most restrictive mode consistent with control system operational requirements.
- **Configuration for Least Functionality**: The organization configures the control system to provide only essential capabilities and specifically prohibit and/or restrict the use of functions, ports, protocols, and/or services as defined in an organizationally generated "prohibited and/or restricted" list.
  - *For AMI and HAN systems, configuring for the least functionality is an extremely important security concept. However, as AMI systems become used for functions in addition to just meter reading, following this precept may become more difficult.*
  - *Power system SCADA systems, which are more fixed and tightly managed, should be configured for least functionality.*
- **Factory default authentication**: The organization changes all factory default authentication credentials on control system components and applications upon installation.
  - *Particularly for revenue-grade meters, certificates and/or security keys must be changed from the vendor's factory keys to the user's keys without loss of security during the transition.*

2.7 Strategic Planning

The purpose of strategic planning is to maintain optimal operations and to prevent or recover from undesirable interruptions to control system operation. Interruptions may take the form of a natural disaster (hurricane, tornado, earthquake, flood, etc.), an unintentional manmade event (accidental equipment damage, fire or explosion, operator error, etc.), an intentional manmade event (attack by bomb, firearm or vandalism, hacker or malware, etc.), or an equipment failure. The types of planning considered are security planning to prevent undesirable interruptions; continuity of operations planning to maintain system operation during and after an interruption); and planning to identify mitigation strategies. The continuity of operations planning may also be designated as incident response planning.

- **Control System Security Plan**: The organization develops and implements a security plan for the control system that provides an overview of the security requirements for the system and a description of the security measures in place or planned for meeting those requirements. Designated officials within the organization review and approve the control system security plan.
  - *A security plan for AMI systems should include both the security measures which are in place, as well as the actions that should be taken if a security anomaly is detected. These actions may include shutting down all or isolating parts of the AMI system, methods for analyzing anomalous data received from different sources, and control actions to respond to suspected security attacks.*
  - *For critical power system operations which must maintain very high availability, the security plan must also contain methods for coping with security anomalies (inadvertent or deliberate) without requiring critical software applications to be halted or critical equipment to be shut-down.*
  - *Personnel roles and responsibilities, including both security personnel and operational personnel, should be defined for responding to and coping with security anomalies.*
  - *Security plans for HAN environments may focus more on containing security attacks rather than providing high availability. However, depending upon the functionality of the HAN equipment, the vendors and integrators of that equipment may develop similar security plans for their equipment within the HAN environment.*
- **Interruption Identification and Classification**: The organization identifies potential interruptions and classifies them as to “cause,” “effects,” and “likelihood” (*the equivalent of “vulnerabilities”, “impacts”, and “probability” used in security risk assessment),* so that a proper response can be formulated for each potential incident. The organization determines the impact to each system and the consequences associated with loss of one or more of the control systems. Proactive measurements to automatically identify attacks during their early stages are determined.
  - *Impacts, and the likelihood of those impacts, are the key for determining the level and type of security measures that are warranted for PRM systems. However, the impact should not be just from the “loss of one or more of the control systems”, but also on the loss or corruption of the **information** flowing between the control systems.*
- **Risk Assessment: Testing, Investigating, Analyzing, Correcting, and Updating**: The organization *should periodically perform risk assessments for all critical functions, including* regularly testing of security plans to validate the control system objectives, investigation and analysis of control system incidents in the planning process, and implementing corrective actions. The organization regularly, at prescribed frequencies, reviews the security plan for the control system and revises the plan to address

system/organizational changes or problems identified during system security plan implementation or security controls assessment.

- *Risk assessment is critical for PRM systems, and should be carried out periodically in order to re-assess situations as systems expand and mature, and as potential threats and vulnerabilities are better understood.*
- *Because PRM systems and functionality are so interconnected, the effects of cascading events and cumulative impacts (e.g." for want of a nail … a kingdom was lost") must become part of the risk assessment.*

2.8 System and Communication Protection

System and communication protection consists of steps taken to protect the control system and the communication links between system components from cyber intrusions.

Security measures in control systems must balance the cost of these measures against the probable impact of security breaches. In particular, since high power system reliability and high availability of access are the key requirements in these control systems, too much security in the form of overly burdensome security measures can ultimately be more insecure than moderate security measures.

In addition to traditional IT security mechanisms, the PRM systems themselves should be used to supplement the detection of security anomalies. In particular, PRM systems should use their monitoring and analytic capabilities to assess these security anomalies and to take the most effective coping actions. So, although some separation of functionality (control system managed separately from the security measures) can be seen as the traditional security approach, actually using the control system functionality could be even more beneficial.

- **Information Remnants**: The control system prevents unauthorized or unintended information transfer via shared system resources.
- **Denial-of-Service Protection:** The control system protects against or limits the effects of denial-of-service attacks based on an organization's defined list of types of denial-of-service attacks.
  - *For PRM system equipment that requires high availability, default modes or settings must be designed into the equipment to take effect if there is a loss of communications or a loss of timely information. No equipment that impacts power system operations or other sensitive activities should be allowed to rely on 100% availability or accuracy of external information.*
  - *For power system operational systems, denial of service attacks, whether deliberate or inadvertent, are the most damaging security attacks, since high availability is critical to high power system reliability. In many systems, redundancy is built into the configuration such that no single point of failure affects critical functions. However, there must be a balance between protecting against denial-of-service and still allowing operations to use alternate means during power system – or information system – emergencies.*
  - *For some HAN functions, such as those involved in demand response and the management of DER and PEV equipment, protection against denial-of-service can*

also be critical. For these, the same level of redundancy and/or alternate methods used in power system operations may be applicable.

- **Resource Priority**: The control system limits the use of resources by priority.
  - *Most denial-of-service attacks are caused by resource exhaustion. For AMI systems with millions of nodes, prioritizing and managing resources to avoid inadvertent denial-of-service attacks is one of the most difficult tasks as different requirements at different times and during different situations stress different resources.*
  - *For power system operations, appropriate resource prioritization is also critical. If key information cannot be received and processed by a SCADA system during a power system problem, then the system or the operator cannot take appropriate action, possibly leading to reduced power system reliability.*
  - *HAN systems are, by their nature, required to be more loosely coupled than other PRM systems, since they are usually under the management of their owner. Therefore, the standards for handling priorities and interactions between systems and equipment in the HAN environment must be very clearly defined to avoid resource exhaustion during critical interactions.*
- **Boundary Protection:** The organization defines the external boundary(ies) of the control system. Procedural and policy security functions define the operational system boundary, the strength required of the boundary, and the respective barriers to unauthorized access and control of system assets and components. The control system monitors and manages communications at the operational system boundary and at key internal boundaries within the system.
  - *For PRM systems, boundary monitoring (also termed network and system management) should become part of their monitoring requirements, since often they can perform this boundary protection with existing capabilities.*
- **Communication Integrity**: The control system design and implementation protects the integrity of electronically communicated information.
  - *For PRM systems, integrity of the information exchanged is vital for almost all interactions, since compromising that integrity could result in decreased power system reliability and/or financial impacts to utilities or customers. Therefore, information should be checked across interfaces for unauthorized modification, reasonability, and errors.*
- **Communication Confidentiality**: The control system design and implementation protects the confidentiality of communicated information where necessary.
  - *For power system operations, confidentiality is generally less important than integrity and availability.*
  - *For AMI and HAN systems, confidentiality of sensitive customer information is a critical privacy issue.*
- **Cryptographic Key Establishment and Management**: When cryptography is required and employed within the control system, the organization establishes and manages

cryptographic keys using automated mechanisms with supporting procedures or manual procedures.

  - *For AMI systems and power system SCADA systems with millions of devices that do not have direct access to certificate authorities, cryptographic key management requires alternate methods. No standards yet exist for this situation, but a new standards effort is to be initiated in the IEC TC57 WG15 to address this challenge.*

- **Public Key Infrastructure Certificates**: The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.
  - *For both AMI systems and power system SCADA systems, if PKI certificates are used, then they should be obtained from approved certificate authorities. However, many interactions in these systems require the use of symmetric secret keys and other key management procedures, often for efficiency and/or access reasons Therefore, PKI should not be the only certificate methodology to be allowed.*

- **System Connections**: All external control system and communication connections are identified and adequately protected from tampering or damage. External access point connections to the control system need to be secured to protect the system. Access points include any externally connected communication end point (for example, dialup modems) terminating at any device within the electronic security perimeter.
  - *For PRM systems, connection points to external systems should be monitored for any security anomalies. In addition, the design of PRM systems should incorporate very strict protections at these connection points, including firewalls, one-way only information flows, call-back dialup modems, store-validate-forward mechanisms, etc.*

- **Message Authenticity**: The control system provides mechanisms to protect the authenticity of device-to-device communications.
  - *For many PRM systems, device-to-device communications are critical to managing local functions or situations. In particular, key management and other security mechanisms for legacy and/or compute-constrained field equipment must be developed before true and effective message authentication can be realized.*
  - *IEC 62351 has specified security standards that should be implemented for any device-to-device interactions that use IEC 61850, IEC 60870-5, or DNP3.*

2.9 Information and Document Management

Information and document management is generally a part of the company records retention and document management system. Digital and hardcopy information associated with the development and execution of a control system is important, sensitive, and needs to be managed. Control system design, operations data and procedures, risk analyses, business impact studies, risk tolerance profiles, etc. contain sensitive company information and needs to be protected. Security measures, philosophy, and implementation strategies are other examples. Additionally, business conditions change and require updated analyses and studies.

- *Information from PRM systems can be sensitive to privacy concerns if it involves personal customer information and/or financial information. Some other information, such as historical information, alarm and event logs, and aggregated customer information should not be lost or altered, but is not necessarily confidential.*

- **Information Handling**: Organization implemented policies and procedures detailing the handling of information are developed and periodically reviewed and updated.
- **Information Exchange**: Formal contractual and confidentiality agreements are established for the exchange of information and software between the organization and external parties.
- **Information and Document Classification**: The organization develops policies and procedures to classify data, including establishing: 1. Retention policies and procedures for both electronic and paper media; 2. Classification policies and methods, (e.g., restricted, classified, general, etc.); 3. Access and control policies, to include sharing, copying, transmittal, and distribution appropriate for the level of protection required; 4. Access to the data based on formally assigned roles and responsibilities for the control system.
  - *For information from AMI and HAN systems, clearly established classifications should be developed for each type of information, with role-based access control to define clearly who (person) or which (software application or system) is permitted to access that information.*
  - *Power system information is generally not as sensitive, unless it has a direct monetary or market value.*

2.10 System Development and Maintenance

Security is most effective when it is designed into the control system and sustained, through effective maintenance, throughout the life cycle of the system and through all future configurations. Maintenance activities encompass appropriate policies and procedures for performing routine and preventive maintenance on the components of a control system. This includes the use of both local and remote maintenance tools and management of maintenance personnel.

- **Legacy System Upgrades**: The organization develops policies and procedures to upgrade existing legacy control systems to include security mitigating measures commensurate with the organization's risk tolerance and the risk to the system and processes controlled. Legacy systems are those control systems currently in place for control of the organization's processes. In some cases, these systems were installed before there was a concern about system security, and hence, security mitigation measures were not included. The organization determines the current configuration of the control system and then provides system upgrades as required to meet the organization's security requirements.
  - *Most AMI and HAN systems are new enough to warrant ensuring that no legacy equipment inhibits the application of security. However, communication traffic constraints of the AMI network may require special or alternate means to handle*

security. For instance, the management of security keys for meters may require special key management techniques, since meters and other end equipment do not have direct access to certificate authorities.

- *HAN systems may have sensitivities to the interactions and impacts of multiple, uncoordinated equipment connected to the communications networks.*
- *Power system equipment is often termed "legacy" equipment given that it was installed years ago and expects to be retained for many years into the future. It is usually uneconomical to justify replacing this equipment just to add security measures. Therefore, alternative compensating security measures must be used for this legacy equipment. These compensating security measures could include extended use of standard SCADA monitoring and control capabilities to detect security anomalies, and/or could expand analysis applications to identify not only power system problems but also security problems.*

- **System Monitoring and Evaluation**: The organization conducts periodic security vulnerability assessments according to the risk management plan. Control systems need to be monitored and evaluated according to the risk management plan periodically to identify vulnerabilities or conditions that might affect the security of a control system. The control system is then updated to address any identified vulnerabilities in accordance with organization's control system maintenance policy. The frequency of these evaluations needs to be based on the organization's risk mitigation policy. Changing security requirements and vulnerabilities necessitate a system review.

- **Backup and Recovery**: The organization makes and secures backups of critical system software, applications, and data for use if the control system operating system software becomes corrupted or destroyed. Control system operating software may be compromised due to an incident or disaster. A copy of the operating system software needs to be made, updated regularly, and stored in a secure environment so that it can be used to restore the control system to normal operations. In many instances, a backup control site can serve this purpose.
  - *Backup of all critical information from PRM systems is vital to ensure that they can cope with deliberate or inadvertent corruption of data or loss of communications.*
  - *Coping with security events by critical PRM functions should be designed around the concept that there be no single point of failure for critical functions.*
  - *Recovery from security events should be planned to take into account the timeliness and availability requirements.*

- **Unplanned System Maintenance**: The organization reviews and follows security requirements for a control system before undertaking any unplanned maintenance activities of control system components (including field devices). Documentation includes the following: 1. The date and time of maintenance; 2. The name of the individual(s) performing the maintenance; 3. The name of the escort, if necessary; 4. A description of the maintenance performed; 5. A list of equipment removed or replaced (including identification numbers, if applicable).

- *Unplanned maintenance of PRM systems, particularly during emergency conditions such as storms and power system outage situations, must be pre-planned as much as possible, must follow established security principles, and must be logged and timestamped as rigorously as possible*

- **Periodic System Maintenance**: The organization schedules, performs, and documents routine preventive and regular maintenance on the components of the control system in accordance with manufacturer or vendor specifications and/or organizational policies and procedures. Maintenance procedures that require the physical removal of any control system component needs to be documented, listing the date, time, reason for removal, estimated date of reinstallation, and name personnel removing components.
  - *Periodic maintenance is critical to AMI systems and power system SCADA systems and is currently performed with great care. However, automated event logging with accurate timestamping of these maintenance activities should be performed as well as ensuring maintenance personnel log their activities rigorously and in a timely manner.*
  - *HAN systems, given that they are under the management of customers, may not be able to meet these maintenance requirements except through recommended practices and possibly automated "maintenance" or security checking.*

- **Remote Maintenance**: The organization authorizes, manages, and monitors remotely executed maintenance and diagnostic activities on the control system. When remote maintenance is completed, the organization (or control system in certain cases) terminates all sessions and remote connections invoked in the performance of that activity. If password-based authentication is used to accomplish remote maintenance, the organization changes the password following each remote maintenance service.
  - *For PRM systems where the remote maintenance uses the normal PRM systems and communication networks (as opposed to the public Internet), the requirement to terminate all connections or changing all passwords may not be necessary. The security requirements for remote maintenance should be reviewed carefully but also should be balanced against practical considerations.*
  - *For HAN systems, the requirement to change passwords or change certificates or keys after remote maintenance or updates should be enforced for all interactions involving public communications and/or 3rd parties.*

2.11 Security Awareness and Training

Physical and cyber control system security awareness is a critical part of control system incident prevention, particularly with regard to social engineering threats. Social engineering is a technique used to manipulate individuals into giving away private information such as passwords. This information can then be used to compromise otherwise secure systems. Implementing a control system security program may change the way personnel access computer programs and applications, so organizations need to design effective training programs based on individuals' roles and responsibilities. Communication vehicles need to be developed to help employees understand why new access and control methods are required and how they can reduce risks and impacts to the organization. Training programs also need to demonstrate management's commitment to cyber and control system security programs. Feedback from staff can be valuable for refining the security program.

- *Security awareness and training is applicable to all PRM systems.*
- *Security awareness and training is vital for new systems, such as AMI and HAN systems where new technologies, new procedures, and new personnel can make people view security training more of an irritant than a necessity.*
- *Security awareness and training – and retraining – is also vital for old systems, such as SCADA systems, where life-long habits and "security by obscurity" attitudes can make people resist change and not take security measures seriously.*

- **Security Awareness**: The organization provides basic security awareness training to all control system users (including managers, senior executives, and contractors) before authorizing access to the system, when required by system changes, and at least annually thereafter. The effectiveness of security awareness training, at the organization level, needs to be reviewed once a year at a minimum.
- **Security Training**: The organization 1. Defines and documents system security roles and responsibilities throughout the system development life cycle; 2. Identifies individuals having system security roles and responsibilities; 3. Provides security-related technical training: (a) before authorizing access to the system or performing assigned duties, (b) when required by system changes, and (c) on an organization-defined frequency thereafter.
- **Security Training Records**: The organization documents, maintains, and monitors individual control system security training activities, including basic security awareness training and specific information and control system security training in accordance with the organization's records retention policy.
- **Contact with Security Groups and Associations**: The organization establishes and maintains contact with security groups and associations to stay up-to-date with the latest recommended security practices, techniques, and technologies and to share current security-related information including threats, vulnerabilities, and incidents.
- **Security Responsibility Testing**: The organization documents and tests the knowledge of personnel on security policies and procedures based on their roles and responsibilities to ensure that they understand their responsibilities in securing the control system.

2.12 Incident Response

Incident response addresses the capability to continue or resume operations of a control system in the event of disruption of normal system operation. Incident response entails the preparation, testing, and maintenance of specific policies and procedures to enable the organization to recover the control system's operational status after the occurrence of a disruption. Disruptions can come from natural disasters such as earthquakes, tornados, floods, or from man made events such as riots, terrorism, or vandalism. The ability for the control system to function after such an event is directly dependent on implementing policies, procedures, training and resources in place ahead of time using the organizations planning process. The security controls that are recommended under the incident response family provide policies and procedures for incident response monitoring, handling, reporting, testing, training, recovery, and reconstitution of the control systems for an organization.

- *For AMI systems, appropriate responses to incidents are vital. For new AMI systems, handling inadvertent or deliberate security incidents may seem less important than just getting the system operating, because currently there are fall-back positions to return to meter readers and other manual methods. But that situation will not last long – very quickly expectations of smooth, continuous, and safe operations will become the norm.*
- *For power system operational systems, management of incidents and continuity of operations often means preventing or minimizing power system outages. This makes this security requirement doubly important. For this reason, many SCADA systems and power system operations planning do already incorporate these procedures into handling power system incidents and SCADA incidents, typically focused on inadvertent equipment failures and mistakes, but expandable to coping with deliberately caused incidents.*

The following procedures for incident handling and response are particularly important for PRM systems.

- **Continuity of Operations Plan**: The organization develops and implements a continuity of operations plan dealing with the overall issue of maintaining or re-establishing production in case of an undesirable interruption for a control system. The plan addresses roles, responsibilities, assigned individuals with contact information, and activities associated with restoring system operations after a disruption or failure.
- **Incident Response Training**: The organization trains personnel in their continuity of operations plan roles and responsibilities with respect to the control system. The organization provides refresher training at least annually. The training covers employees, contractors, and stakeholders in the implementation of the continuity of operations plan.
- **Continuity of Operations Plan Testing**: The organization tests the continuity of operations plan to determine its effectiveness and documents the results. Appropriate officials within the organization review the documented test results and initiate corrective actions if necessary. The organization tests the continuity of operations plan for the control system at least annually, using organization prescribed tests and exercises to determine the plan’s effectiveness and the organization’s readiness to execute the plan.
- **Incident Handling**: The organization implements control system incident handling capabilities for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.
- **Incident Reporting**: The organization promptly reports cyber and control system security incident information to the appropriate authorities.
- **Incident Response Investigation and Analysis**: The organization documents its policies and procedures to show that investigation and analysis of incidents are included in the planning process. The procedures ensure that the control system is capable of providing event data to the proper personnel for analysis and for developing mitigation steps.

- **Corrective Action**: The organization includes processes and mechanisms in the planning to ensure that corrective actions identified as the result of a cyber security incident are fully implemented.
- **Alternate Command/Control Methods**: The organization identifies alternate command/control methods for the control system and initiates necessary agreements to permit the resumption of operations for the safe operation of the control system within an organization-defined time period when the primary system capabilities are unavailable.
- **Alternate Control Center**: The organization identifies an alternate control center, necessary telecommunications, and initiates necessary agreements to permit the resumption of control system operations for critical functions within an organization-prescribed time period when the primary control center is unavailable.
- **Control System Backup**: The organization conducts backups of critical control system information, including state of the user-level and system level information, process formulas, system inventories, etc., contained in the control system, on a regular schedule as defined by the organization, and stores the information at an appropriately secured location.
- **Control System Recovery and Reconstitution**: The organization employs mechanisms with supporting procedures to allow the control system to be recovered and reconstituted to the system's original state after a disruption or failure.
- **Fail-Safe Response**: The control system has the ability to execute an appropriate fail safe procedure upon the loss of communications with the control system or the loss of the control system itself. In the event of a loss of communication between the control system and the operational facilities, the onsite instrumentation needs to be capable of executing a procedure that provides the maximum protection to the controlled infrastructure. For the electric industry, this may be to alert the operator of the failure and then do nothing (e.g., let the electric grid continue to operate).

2.13 Media Protection

The security controls under the media protection family provide policy and procedures for limiting access to media to authorized users. Security measures also exist for labeling media for distribution and handling requirements, as well as storage, transport, sanitization (removal of information from digital media), destruction, and disposal of the media. Media assets include CDs; DVDs; erasable, programmable read-only memory; tapes; printed reports; and documents.

- *These requirements affect PRM systems in a very similar manner to other systems.*
- *For HAN systems, management of media will be the responsibility of the customer*

2.14 System and Information Integrity

Maintaining a control system, including information integrity, increases assurance that sensitive data have neither been modified nor deleted in an unauthorized or undetected manner. The security controls described under the system and information integrity family provide policy and procedure for identifying, reporting, and correcting control system flaws. Controls exist for malicious code detection, spam protection, and tools and techniques. Also provided are controls for receiving security alerts and advisories and the verification of security functions on the control system. In addition, controls within this family detect and protect against unauthorized changes to software and data; restrict data input and output; check the accuracy, completeness, and validity of data; and handle error conditions.

   – *These requirements affect PRM systems in a very similar manner to other systems.*

- **Flaw Remediation**: The organization identifies, reports, and remediates control system flaws (per organizational, legal, and/or regulatory policies).

   – *For most PRM systems, contracts with vendors or system integrators cover the remediation of “flaws” in which the delivered system fails to provide the contractual functionality and/or performance.*

- **Malicious Code Protection**: The control system employs malicious code protection. The organization employs malicious code protection mechanisms at critical control system entry and exit points (e.g., firewalls, web servers, proxy servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network. The organization uses the malicious code protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses, spyware). The organization updates malicious code protection mechanisms (including the latest virus definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures.

   – *PRM systems should incorporate commercially available malicious code protection for those components that use standard PC or microprocessor hardware/firmware. Special code protection should be provided with equipment that cannot utilize commercially available products.*

   – *Updating virus definitions or other malicious code protection software is generally not possible for those PRM systems or equipment such as meters that must be re-certified. For these, only critical updates may be required.*

- **System Monitoring Tools and Techniques**: The organization employs tools and techniques to monitor security events and system activities on the control system, detect attacks, and provide identification of unauthorized use of the system.

   – *In addition to traditional IT security intrusion detection and security monitoring, PRM systems should expand their own monitoring and alarming capabilities to include detection and analysis of security anomalies.*

- **Security Alerts and Advisories**: The organization: 1. Receives control system security alerts/advisories regularly and in response to system-based occurrences; 2. Issues alerts/advisories to appropriate personnel; 3. Takes appropriate actions in response.

- **Security Functionality Verification**: The organization verifies the correct operation of security functions within the control system upon system startup and restart; upon command by user with appropriate privilege; periodically; and/or at defined time periods. The control system notifies the system administrator when anomalies are discovered.
- **Software and Information Integrity**: The control system monitors and detects unauthorized changes to software and information.
  - *PRM systems should use RBAC techniques for both personnel access and software application access to software and information.*
- **Spam Protection**: The control system implements spam protection. The organization employs spam protection mechanisms at critical control system entry points (e.g., firewalls, electronic mail servers, remote-access servers) and at workstations, servers, and/or mobile computing devices on the network.
  - *Spam protection may apply only to certain PRM systems, specifically any HAN systems that utilize the public Internet.*
- **Information Input Restrictions**: The organization implements security measures to restrict information input to the control system to authorized personnel only.
  - *PRM systems should use RBAC techniques for input from both personnel and from software application.*
- **Information Input Accuracy, Completeness, Validity, and Authenticity**: The control system employs mechanisms to check information for accuracy, completeness, validity, and authenticity. Organization checks for accuracy, completeness, validity, and authenticity of information are accomplished as close to the point of origin as possible. Rules for checking the valid syntax of control system inputs (e.g., character set, length, numerical range, acceptable values) are in place to ensure that inputs match specified definitions for format and content. Inputs passed to interpreters are pre-screened to ensure the content is not unintentionally interpreted as commands. The extent to which the control system is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements.
  - *It is vital that PRM systems validate input from human users, equipment measurements, and software applications as much as is feasible. This validation should include data "reasonability" as well as, where warranted, analysis to detect any inconsistencies in data from different sources. For instance, power flow based analysis should be used for power system measurements, including for DER equipment within HAN systems.*
- **Error Handling**: The system identifies error conditions, generates error messages that provide information necessary for corrective actions without revealing potentially harmful information that could be exploited by adversaries, reveals error messages only to authorized personnel, and prohibits inclusion of sensitive information in error logs or associated administrative messages.
- **Information Output Handling and Retention**: The organization handles and retains output from the control system in accordance with applicable laws, regulations,

standards, and organizational policy, as well as operational requirements of the control process.

- **Predictable Failure Prevention**: The organization protects the system from harm by considering mean time to failure for an organization-defined list of system components in specific environments of operation, and provides substitute system components, when needed, and a mechanism to exchange active and standby roles of the components.

2.15 Access Control

The focus of access control is ensuring that resources are only accessed by the appropriate personnel and that personnel are correctly identified. The first step in access control is creating access control lists with access privileges for personnel. The next step is to implement security mechanisms to enforce the access control lists. Mechanisms also need to be placed to monitor access activities for inappropriate activity. The access control lists need to be managed through adding, altering, and removing access rights as necessary.

Identification and authentication is the process of verifying the identity of a user, process, or device, as a prerequisite for granting access to resources in a control system. Identification could be a password, a token, or a fingerprint. Authentication is the challenge process to prove (validate) the identification provided. An example would be using a fingerprint (identification) to access a computer via a biometric device (authentication). The biometric device authenticates the identity of the fingerprint.

- – *For PRM systems, access control must also apply to software applications that require access within their own system and across interfaces to other systems. In particular, access privileges must be settable down to the data item level, not just to the system or application or database level.*
- – *Role-Based Access Control (RBAC) (see IEC 62351-8) should be used for all control systems, covering personnel AND software applications as "Users", while separating these Users from the different roles they play. The roles will be assigned privileges, not Users.*

- **Account Management**: The organization manages system accounts, including:
  - ➢ Identifying account types (i.e., individual, group, and system)
  - ➢ Establishing conditions for group membership
  - ➢ Identifying authorized users of the system and specifying access rights and privileges
  - ➢ Requiring appropriate approvals for requests to establish accounts
  - ➢ Authorizing, establishing, activating, modifying, disabling, and removing accounts
  - ➢ Reviewing accounts on a defined frequency
  - ➢ Specifically authorizing and monitoring the use of guest/anonymous accounts
  - ➢ Notifying account managers when system users are terminated, transferred, or system usage or need-to-know/need-to-share changes

- ➢ Granting access to the system based on a valid need-to-know or need-to-share that is determined by assigned official duties and satisfying all personnel security criteria and intended system usage.

– *Role-Based Access Control should be used which identifies Users separately from the Roles they play. The term "Users" must encompass software applications as well as personnel. In addition, "roles" should be established rather than "groups" to ensure clarity when the privileges are assigned to a role.*

- **Access Enforcement**: The control system enforces assigned authorizations for controlling logical access to the system in accordance with applicable policy. Access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, and cryptography) are employed by organizations to control access to the control system. **The organization considers the implementation of a controlled, audited, and manual override of automated mechanisms in the event of emergencies or other serious events.**

  – *For PRM systems, manual override of automated mechanisms, including security mechanisms, must be permitted for emergency conditions particularly where power system reliability is at stake.*

- **Least Privilege**: The organization employs the concept of least privilege, limiting authorized access for users (and processes acting on behalf of users) as necessary, to accomplish assigned tasks.

  – *For PRM systems, the concept of least privilege should be applied to all role-based access control privileges, including software application privileges as well as User privileges.*

- **Device Identification and Authentication**: The system uniquely identifies and authenticates an organization-defined list of devices before establishing a connection. The devices requiring unique identification and authentication may be defined by type, by specific device, or by a combination of type and device as deemed appropriate by the organization. The system typically uses either shared known information (e.g., MAC or Transmission Control Protocol/IP [TCP/IP] addresses) or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP] or a Radius server with EAP-Transport Layer Security authentication) to identify and authenticate devices on local and/or wide area networks. The required strength of the device authentication mechanism is determined by the security categorization of the system with higher impact levels requiring stronger authentication.

  – *This requirement for authentication of device is not adequate for PRM systems – access privileges must be not only at the device level, but at the individual data or data type level.*

  – *The method for authentication of the device must reflect the capabilities of the protocols used for connection, so the ones identified here may or may not be possible.*

- **Information Flow Enforcement**: The control system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.
  - *For PRM systems, the authorization of information flows must reflect RBAC requirements and must be not only between systems, but at a data or data type level.*
- **Passwords**: The organization develops and enforces policies and procedures for control system users concerning the generation and use of passwords. These policies stipulate rules of complexity, based on the criticality level of the systems to be accessed.
  - Default passwords of applications, operating systems, database management systems, or other programs must be changed immediately after installation.
  - The organization replaces default usernames whenever possible. Passwords need to be allocated, protected, and used based on the criticality level of the systems to be accessed.
  - The organization develops policies that stipulate the complexity (minimum/maximum length, combination of lower/upper case, numerals, special characters, etc.) level of the password for each criticality level. Short or easily guessed passwords are prohibited. Passwords can be a means of system protection when properly generated and used. Although passwords are not advisable in all control system applications, there are some cases where they are of benefit such as for remote access. These passwords are developed to meet defined metrics.
  - Good security practices need to be followed in the generation of passwords. Passwords should not easily be associated with the user or the organization and follow appropriate complexity rules. Initial or default passwords are changed immediately on first login. Following generation, passwords are not sent across any network unless protected by encryption or salted cryptographic hash specifically designed to prevent replay attacks.
  - Passwords need to be transferred to the user via secure media, and the recipient must be verified. The logon ID and password are never combined in the same communication.
  - The authority to keep and change high-level passwords is given to a trusted employee who is available during emergencies.
  - A log for master passwords needs to be maintained separately from the control system, possibly in a notebook in a vault or safe.
  - Passwords need to be changed regularly and expire when the user leaves the organization or after an extended period of inactivity.
  - Users are responsible for their passwords and are instructed not to share them or write them down, and need to be aware of their surroundings when entering passwords. If the operating system supports encryption, stored passwords are encrypted. Passwords are not to be embedded into tools, source code, scripts, aliases, or shortcuts.
  - *Password management for all PRM systems is critical to security.*

  - *For systems and equipment on HAN networks, passwords must be required, although some of the management requirements may not be enforceable other than as recommendations since the customer is ultimately in charge.*

- **Unsuccessful Login Attempts**: The system enforces a limit of an organization-defined number of consecutive invalid access attempts by a user during an organization-defined time period, and automatically locks the account/node for an organization-defined time period and delays the next login prompt according to an organization-defined delay algorithm when the maximum number of unsuccessful attempts is exceeded.
  - *For PRM systems in general, the lockout time period should reflect the criticality of the affected systems and the impact of a mistaken lockout.*
  - *For systems on HAN networks, the customer should be able to manage these login characteristics.*

- **Remote Session Termination**: The system terminates a network connection at the end of a session or after an organization-defined time period of inactivity. This control applies to both organization-controlled networks and non-organization-controlled networks. The organization-defined time period of inactivity may, as the organization deems necessary, be a set of time periods by type of network access or for specific accesses in accordance with an organizational assessment of risk.
  - *For AMI systems and power system operational systems, this security requirement does not apply for most normal remote sessions since these are usually considered as permanent connections.*
  - *For engineering system connections to remote equipment, remote session termination requirements should be implemented.*
  - *For HAN systems, any network connections using public or private external networks, remote session termination requirements should be implemented.*

- **Remote Access**: The organization authorizes, monitors, and manages all methods of remote access to the control system. Appropriate authentication methods are needed to adequately secure remote access.
  - *PRM systems should use RBAC for remote access management and authentication.*

- **Access Control for Portable and Mobile Devices**: The organization:
  - Establishes usage restrictions and implementation guidance for organization-controlled mobile devices
  - Authorizes connection of mobile devices to organizational systems
  - Monitors for unauthorized connections of mobile devices to organizational systems
  - Enforces requirements for the connection of mobile devices to organizational systems
  - Disables system functionality that provides the capability for automatic execution of code on removable media without user direction

  - ➢ Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures
  - ➢ Applies specified measures to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.
- – *Engineering and power system operational systems which communicate with mobile devices must implement these requirements.*
- – *HAN systems must also implement these requirements for systems and equipment that are considered external to the HAN, but interface with HAN systems.*

- **Wireless Access Restrictions**: The organization establishes use restrictions and implementation guidance for wireless technologies and authorizes, monitors, and manages wireless access to the control system.

2.16 Audit and Accountability

Periodic audits and logging of the control system need to be implemented to validate that the security mechanisms present during system validation testing are still installed and operating correctly. These security audits review and examine a system's records and activities to determine the adequacy of system security controls and to ensure compliance with established security policy and procedures. Audits also are used to detect breaches in security services through examination of system logs. Logging is necessary for anomaly detection as well as forensic analysis.

- **Auditable Events**: The organization:
  - ➢ Determines, based on a risk assessment in conjunction with mission/business needs, which system-related events require auditing (e.g., an organization-defined list of auditable events and frequency of [or situation requiring] auditing for each identified auditable event)
  - ➢ Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events
  - ➢ Ensures that auditable events are adequate to support after-the-fact investigations of security incidents
  - ➢ Adjusts, as necessary, the events to be audited within the system based on current threat information and ongoing assessments of risk.
- – *For PRM systems, alarm and event logging is usually available as part of the normal functions. This logging capability should be expanded to include security-related events which should be audited.*
- – *For systems and software applications connected to the HAN, logging of events, including security-related events, should become part of their specifications, particularly if these systems are monitoring, controlling, and managing equipment like DER and PEV equipment.*

- **Time Stamps**: The system uses internal system clocks to generate time stamps for audit records. The system synchronizes internal system clocks on an organization-defined frequency.
  - *For most PRM systems, time synchronization needs to be at the sub-second level in order to capture the true sequence of rapid events occurring in different locations with different types of systems.*
  - *For HAN systems involving DR, DER, PEV, or other energy-related equipment, time stamp accuracy should also be at the sub-second level.*

2.17 Monitoring and Reviewing Control System Security Policy

Monitoring and reviewing the performance of an organization's cyber and control system security policy provides the organization the ability to evaluate the performance of their security program. Internal checking methods, such as compliance audits and incident investigations, allow the company to determine the effectiveness of the security program and whether it is operating according to expectations. Finally, through a continuous improvement process, the organization's senior leaders regularly review compliance information on the security program, developed through the audit and corrective action process, and any deviations from the goals, targets, and objectives set in the planning process. If deviations or nonconformance exist, it may be necessary to revisit the original assumptions and implement appropriate corrective actions.

- *These requirements affect PRM systems in a very similar manner to other systems.*

2.18 Risk Management and Assessment

Risk management planning is a key aspect of ensuring that the processes and technical means of securing control systems have fully addressed the risks and vulnerabilities in the system.

An organization identifies and classifies risks to develop appropriate security measures. Risk identification and classification involves security assessments of control system and interconnections to identify critical components and any areas weak in security. The risk identification and classification process is continually performed to monitor the control system's compliance status. A documented plan is developed on how the organization will strive to stay in compliance within acceptable risk.

A comprehensive organization risk assessment process is implemented and periodically executed. Assets are categorized into security levels based on the level of security is necessary for each asset to be sufficiently protected. Risk is assessed across the organization by determining the likelihood of potential threats and cost if the threat is realized. Control system vulnerabilities need to be recognized and documented.

- **Risk Management Plan**: The organization develops a risk management plan. A senior organization official reviews and approves the risk management plan.
  - *For AMI and power operations systems, this simple sounding security requirement actually takes tremendous effort due to the complexity of these systems and the very*

large number of stakeholders, systems, software applications, equipment, and networks involved.

- *For systems on HAN networks, the risk assessment must be done on a product-by-product basis, since there will not be any single authority to manage a risk assessment of the entire HAN network.*

- **Security Assessments**: The organization assesses the security controls in the system on an organization-defined frequency, at least annually, to determine the extent the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system, and produces a security assessment report that documents the results of the assessment.
  - *For systems on HAN networks, this requirement may not be possible on a per-HAN basis, but will need to be approached on a product-by-product basis, much as there are security updates to Microsoft operating systems periodically as they find security flaws in their software.*
- **Control System Connections**: The organization authorizes all connections from the system to other systems outside the authorization boundary through the use of system connection agreements, documents the system connections and associated security requirements for each connection, and monitors the system connections on an ongoing basis verifying enforcement of documented security requirements.
  - *For systems on HAN networks, this requirement may not be possible on a per-HAN basis, but will need to be approached on a product-by-product basis. In particular, vendors of HAN networks should require secured control system connections, using certificates or keys for access, and complete timestamped logging of all connections and interactions.*
- **Continuous Monitoring**: The organization monitors the security mechanisms in the control system on an ongoing basis. Those security mechanisms that are volatile or critical to protecting the control system are assessed at least annually. All other security mechanisms are assessed at least once during the control system's 3-year accreditation cycle.
  - *Continuous monitoring of security should be required for all PRM systems. However, the timeframes for assessment and accreditation should be part of the Risk Management and/or Security Policy of the organization, not mandated specifically.*
  - *For systems on HAN networks, the annual assessment and the 3-year accreditation requirement may not be feasible. Other mechanisms for assessing security measures must be developed product-by-product according to HAN recommendations (which will need to be developed).*
- **Risk Assessment**: The organization conducts assessments of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and systems that support the operations and assets of the organization, and updates risk assessments on an organization-defined frequency or whenever significant changes occur to the system or

environment of operation, or other conditions that may impact the security state of the system.

– *Risk assessment of PRM systems primarily involves determining the likelihood of a threat occurring, times the likelihood of a vulnerability, times the probable impact of a security breach. Given the complexity of PRM systems, the unique configurations of implementations, and the possibility of cascading impacts, no simple risk assessment process is possible. Therefore, this "checklist" of key security controls should be used to develop security requirements for products, systems, equipment, and organizations.*

3. Security Requirements for AMI Interface Categories

3.1 Characteristics-Based Interface Categories for Defining Security Requirements

3.1.1 Interface Characteristics: Requirements, Constraints, and Issues Defining Interfaces

At the most basic level, security requirements are just the need for confidentiality, integrity, and availability (CIA). But the feasibility and cost-effectiveness of different security measures to meet these basic requirements are really affected by the technical constraints and organizational issues of the interfaces and systems. ***Although actual security measures must reflect the real-world of specific implementations, these security-related categories can be helpful as examples, guidelines, and/or checklists of security requirements to help utilities specify security requirements and to assist vendors and integrators as they design, implement, and maintain secure systems***.

Table 1 is the list of interface characteristics: the types of requirements, constraints, and issues (usually as a result of the balancing of cost versus security) that can help determine the key types of security requirements for the interfaces and the actors (systems, equipment, databases, etc.). These interface characteristics may therefore influence, limit, or otherwise impact the types, layers, thoroughness, and/or effectiveness of security measures for the associated actors and interface.

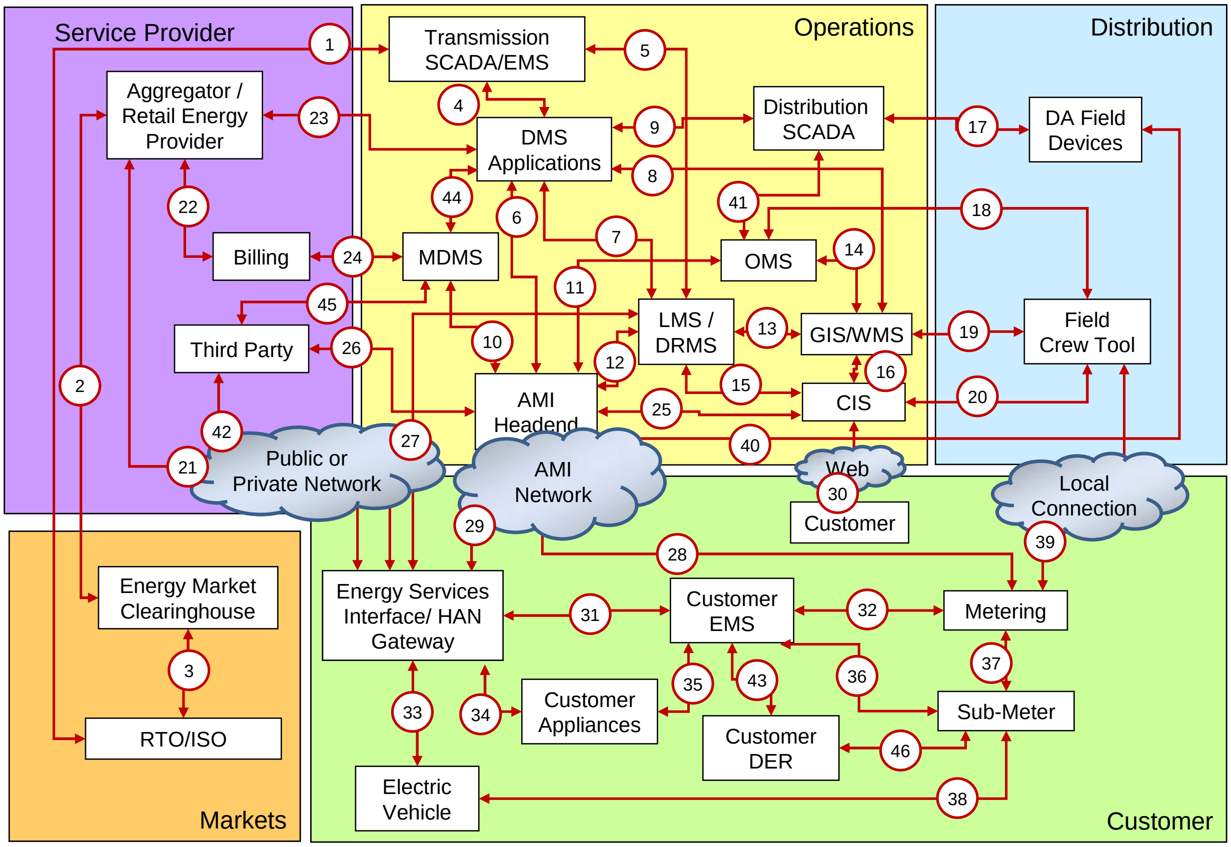
Table 1: Interface Characteristics: Requirements, Constraints, and Issues

Requirement, Constraint, or Issue	Description
Cst-1: High requirement for confidentiality and/or privacy	which necessitates or strongly influences the types of security measures required.
Cst-2: High requirement for integrity and/or accuracy of data	which influences not only the types of typical security measures, but also necessitates strong accuracy and error checking.
Cst-3: High requirement for availability	which influences system design, network configuration, and procedures for achieving the necessary availability
Cst-4: Low bandwidth of communications channels	which limits the types of security measures which could be employed per channel.
Cst-5: Microprocessor constraints on memory and compute capabilities	which limits the types of security measures which could be employed.
Cst-6: Wireless media	which can pose certain types of additional security challenges.
Cst-7: Immature or proprietary protocols	which may not be adequately tested either against inadvertent compromises or deliberate attacks.
Cst-8: Cross-organizational interactions	which limit trust and compatibility of security policies and measures, including the use of out-sourced services and leased networks.
Cst-9: Real-time operational requirements	which entail short acceptable time latencies, and limit the choices for stopping or mitigating on-going attacks.

Requirement, Constraint, or Issue	Description
Cst-10: Legacy end-devices and systems	which limit the types, thoroughness, or effectiveness of different security measures which could be employed.
Cst-11: Legacy communication protocols	which limit the types, thoroughness, or effectiveness of different security measures which could be employed.
Cst-12: Insecure locations	which cannot be made more secure due to their physical environment or ownership.
Cst-13: Key management for large numbers of devices	which can limit the methods for deploying and revoking keys.
Cst-14: Patch and update management constraints for sensitive devices	which limits the frequency of updating security patches.
Cst-15: Unknown or rapidly changing types of interactions	which complicate the decisions on the types and severity of security threats and impacts.
Cst-16: Environmental and physical access constraints	which limit the types of security measures, particularly physical security.
Cst-17: Legal constraints limiting security measures	which constrain what security could be employed, such as wiretapping of suspected hackers or blocking all 3rd party access.
Cst-18: Lack of security-consciousness in personnel	which can cause inadvertent by-passing of security measures and can limit the number of properly trained personnel to manage and secure resources. This includes the lack of any security training of most customers.
Cst-19: Negative public image or fears	which can limit what functions are deployed and the types of security measures mandated or regulated.
Cst-20: Security budgetary constraints	which limit the development of good security policies and procedures, limit the security training of personnel, and constrain the types of security tools and services to properly monitor, test, and protect the resources.
Cst-21: Sharing of known security vulnerabilities and security incidents limited by legal and/or regulatory factors	which can cause vulnerabilities to perpetuate.
Cst-22: Novel business functions with unknown ramifications from security breaches	which can either lead to unwarranted, burdensome security measures or, more likely, inadequate security measures.
Cst-23: Lack of standards across interfaces	which can lead to ad hoc engineering, difficulty in testing between vendor systems, and increased likelihood of security holes.

3.1.2 AMI System Diagram

The AMI System diagram used to identify the AMI interfaces is shown in Figure 1.



AMI Systems Use Cases: Actors, Logical Interfaces, and Networks

AMI: Advanced Metering Infrastructure
SCADA: Supervisory Control and Data Acquisition
WMS: Work Management System
DRMS: Demand Response Management System
MDMS: Meter Data Management System
DMS: Distribution Management System
EMS: Energy Management System
LMS: Load Management System
GIS: Geographic Information System
CIS: Customer Information System
OMS: Outage Management System

Figure 1: AMI System Actors, Logical Interfaces, and Networks

3.1.3 Security-Related Interface Categories

Many interfaces are similar in their security-related characteristics, and can therefore be categorized together as a means to simplify the identification of the appropriate security measures. Therefore, security-related interface categories were defined based on known critical security requirements, technological constraints, organizational structures, and any legal or regulatory concerns that could affect the types of security requirements. The Interface Categories are described with examples and AMI interface assignments in Table 2.

Although different implementation designs and configurations may not fit exactly into the interface category associated with them, nonetheless, this categorization can help as a checklist.

Table 2: Security-Related Interface Categories

Security-Related Interface Categories	Examples	AMI Interfaces
1a. Control systems with high data accuracy requirements and high availability, as well as media and/or compute constraints	• Between SCADA and transmission legacy field equipment • Between SCADA and legacy but critical distribution equipment • Between protective relays	a. AMI 17
1b. Control systems with high data accuracy requirements, as well as media and/or compute constraints, but not high availability	• Between SCADA and legacy but less critical field equipment using the AMI network • Between distribution field equipment	a. AMI 40
2. Control systems with no bandwidth constraints (WAN) but are in different organizations	• Between an RTO/ISO EMS and a utility energy management system	a. AMI 1 b. AMI 4 c. AMI 5 d. AMI 6 e. AMI 7 f. AMI 44
3. Control systems within the same organization with no bandwidth constraints	• Between multiple DMS systems belonging to the same utility • Between SCADA system and transmission substation automation systems	a. AMI 9 b. AMI 41
4. Back office systems under common management authority	• Between a Customer Information System and a Meter Data Management System	a. AMI 10 b. AMI 11 c. AMI 12 d. AMI 16 e. AMI 22 f. AMI 25
5. Back office systems not under common management authority	• Between a third party billing system and a utility meter data management system	a. AMI 23 b. AMI 24 c. AMI 26 d. AMI 45
6. B2B connections usually involving financial or market transactions	• Between a Retail aggregator and an Energy Clearinghouse	a. AMI 2 b. AMI 3
7. Interfaces between control systems and non-control systems	• Between a Geographic Information System and a Load Management/Demand Response System	a. AMI 8 b. AMI 13 c. AMI 14 d. AMI 15
8. Sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements	• Between temperature sensor on a transformer and its receiver	*a. (None)*

Security-Related Interface Categories	Examples	AMI Interfaces
9. Interfaces between sensor networks and control systems	• Between a sensor receiver and the substation master	a. *(None)*
10. Interfaces that use the AMI network	• Between MDMS and meters • Between LMS/DRMS and Customer EMS • Between DMS Applications and Customer DER • Between DMS Applications and DA Field Equipment	a. AMI 28 b. AMI 29 c. AMI-40
11. Interfaces that use customer (residential, commercial, and industrial) site networks such as HANs and BANs	• Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and PEV	a. AMI 31 b. AMI 32 c. AMI 33 d. AMI 34 e. AMI 35 f. AMI 36 g. AMI 43 h. AMI 46
12. Interface to the Customer Site	• Between Customer and CIS Web site • Between Third Party and HAN Gateway	a. AMI 21 b. AMI 27 c. AMI 30 d. AMI 42
13. Mobile Field Crew interfaces	• Between field crews and GIS • Between field crews and substation equipment	a. AMI 18 b. AMI 19 c. AMI 20 d. AMI 39
14. Metering interface	• Between sub-meter to meter • Between PEV meter to Energy Service Provider	a. AMI 28 b. AMI 37 c. AMI 38
15. Decision support interfaces	• Between Wide Area Measurement System (WAMS) and ISO/RTO	a. *(None)*
16. Engineering systems downloading field equipment settings, uploading logs, and maintenance	• Between engineering and substation relaying equipment for relay settings • Between engineering and pole-top equipment for maintenance	a. *(None)*

3.1.4 Definition of Categories by Interface Characteristics

The security-related interface categories described in Table 2 are defined by the interface characteristics described in Table 1: these category definitions are shown in the Table 3 spreadsheet.

Table 3: Security-Related Interface Categories, Defined by Interface Characteristics

Security-Related Interface Categories, Defined by Interface Characteristics: Critical Security Requirements, Technical Constraints, and Organizational Issues

Requirements, Constraints, and Issues Security-Related Categories for Interfaces	Cst-1: High requirement for confidentiality and/or privacy	Cst-2: High requirement for integrity and/or accuracy of data	Cst-3: High requirement for availability	Cst-4: Low bandwidth of communications channels	Cst-5: Microprocessor constraints on memory and compute	Cst-6: Wireless media	Cst-7: Immature or proprietary protocols	Cst-8: Cross-organizational interactions	Cst-9: Real-time operational requirements	Cst-10: Legacy end-devices and systems	Cst-11: Legacy communication protocols	Cst-12: Insecure locations	Cst-13: Key management for large numbers of devices	Cst-14: Patch and update manage-ment constraints for sensitive	Cst-15: Unknown or rapidly changing types of interactions	Cst-16: Environmental and physical access constraints	Cst-17: Legal constraints limiting security measures	Cst-18: Lack of security-consciousness in personnel	Cst-19: Negative public image or fears	Cst-20: Security budgetary constraints	Cst-21: Sharing of known security vulnerabilities and incidents limited	Cst-22: Novel business functions with unknown ramifications	Cst-23: Lack of standards across interfaces
1a. Control systems with high data accuracy and high availability, as well as compute constraints (e.g. transmission)		x	x	x	x				x	x	x	x	x	x		x		x		x	x		x
1b. Control systems with high data accuracy without high availability, as well as compute constraints (e.g. distribution)		x		x	x				x	x	x	x	x	x		x		x		x	x		x
2. Control systems with no compute or bandwidth constraints (WAN) but are in different organizations		x	x					x	x		x						x	x		x	x		x
3. Control systems within the same organization with no compute or bandwidth constraints		x	x						x		x							x		x	x		x
4. Back office systems under common management authority	x	x																x		x			x
5. Back office systems not under common management authority	x	x						x									x	x		x	x		x
6. B2B connections usually involving financial or market transactions	x	x						x							x		x		x		x	x	
7. Interfaces between control systems and non-control systems							x	x							x					x			x
8. Sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements				x	x	x	x		x	x	x					x							
9. Interfaces between sensor networks and control systems		x	x	x	x	x			x	x	x												
10. Interfaces that use the AMI network	x			x	x	x	x	x			x	x	x		x	x	x		x	x	x	x	x
11. Interfaces that use customer (residential, commercial, and industrial) site networks such as HANs and BANs						x	x	x				x	x		x	x	x	x	x			x	x
12. Interface to the Customer Site	x					x		x				x	x		x	x	x	x	x			x	x
13. Mobile Field Crew interfaces		x		x		x	x		x			x						x					x
14. Metering interface	x	x		x	x	x	x	x		x	x	x	x	x		x	x	x	x	x			x
15. Decision support interfaces	x	x			x			x	x									x				x	
16. Engineering systems downloading field equipment settings, uploading logs, and maintenance		x		x	x					x	x	x	x	x		x		x		x	x		x

3.2 Security Requirements Applicable to Specific Interface Categories

At one level, all security requirements are pertinent to all interfaces. But this is usually not economically or practically feasible – for actual implementations, a balance needs to be struck between the cost (financial, maintenance effort, and performance impacts) of implementing security measures and the cost (financial, legal, and societal impacts) of security breaches.

So only the key security requirements, corresponding to the interface characteristics and possible types of impacts, are identified for each category. Clearly specific implementations with different types of equipment and different environments will vary on which vulnerabilities and requirements are the most important, but these categorizations can provide guidelines.

Acting as an excellent checklist of security requirements, the DHS "Catalog of Security Controls" (DHS-CSC) are used to identify most of the key security requirements. In addition, where applicable, traditional power system management technologies are identified as providing methods for meeting some of the security requirements.

3.2.1 General DHS Security Requirements

At the broadest level, some DHS security requirements apply to all Interface Categories, including:

- Security Policies *(DHS-CSC 2.1)*
- Organizational Security *(DHS-CSC 2.2)*
- Personnel Security *(DHS-CSC 2.3)*
- System and Services Acquisition *(DHS-CSC 2.5)*
- Strategic Planning *(DHS-CSC 2.7)*
- Information and Document Management *(DHS-CSC 2.9)*
- System Development and Maintenance *(DHS-CSC 2.10)*
- Security Awareness and Training *(DHS-CSC 2.11)*
- Media Protection *(DHS-CSC 2.13)*
- Monitoring and Reviewing Control System Security Policy *(DHS-CSC 2.17)*
- Risk Management and Assessment *(DHS-CSC 2.18)*

Some security requirements, although still applicable for all Interface Categories (particularly the policy requirements), have special implications, issues, and possible solutions that are related to individual Interface Categories, and can be considered as high priority security requirements. These special implications impact the following security requirements, and are discussed in the following sections:

- Physical and Environmental Security *(DHS-CSC 2.4)*
- Configuration Management *(DHS-CSC 2.6)*

- System and Communication Protection *(DHS-CSC 2.8)*
- Incident Response *(DHS-CSC 2.12)*
- System and Information Integrity *(DHS-CSC 2.14)*
- Access Control *(DHS-CSC 2.15)*
- Audit and Accountability *(DHS-CSC 2.16)*

3.2.2 Interface Categories Specifically Applicable to AMI Systems

Although business processes involving AMI systems also impact most of the Interface Categories, some Interface Categories are of particular importance:

- Interface Category 1a: Control Systems with High Data Accuracy Requirements and High Availability, as well as Media and/or Compute Constraints
- Interface Category 1b: Control Systems with High Data Accuracy Requirements, as well as Media and/or Compute Constraints, but Not High Availability
- Interface Category 10: Interfaces That Use the AMI Network to the Customer Site
- Interface Category 14: Metering Interfaces

3.2.3 Interface Category 1a: Control Systems with High Data Accuracy Requirements and High Availability, as well as Media and/or Compute Constraints

3.2.3.1 Interface Category 1a Characteristics

- Cst-2: High requirement for integrity and/or accuracy of data which influences not only the types of typical security measures, but also necessitates strong accuracy and error checking.
- Cst-3: High requirement for availability which influences system design, network configuration, and procedures for achieving the necessary availability
- Cst-4: Low bandwidth of communications channels which limits the types of security measures which could be employed per channel.
- Cst-5: Microprocessor constraints on memory and compute capabilities which limits the types of security measures which could be employed.
- Cst-9: Real-time operational requirements which entail short acceptable time latencies, and limit the choices for stopping or mitigating on-going attacks.
- Cst-10: Legacy end-devices and systems which limit the types, thoroughness, or effectiveness of different security measures which could be employed.
- Cst-11: Legacy communication protocols which limit the types, thoroughness, or effectiveness of different security measures which could be employed.

- Cst-12: Insecure locations which cannot be made more secure due to their physical environment or ownership.
- Cst-13: Key management for large numbers of devices which can limit the methods for deploying and revoking keys.
- Cst-14: Patch and update management constraints for sensitive devices which limits the frequency of updating security patches.
- Cst-16: Environmental and physical access constraints which limit the types of security measures, particularly physical security.
- Cst-18: Lack of security-consciousness in personnel which can cause inadvertent by-passing of security measures and can limit the number of properly trained personnel to manage and secure resources. This includes the lack of any security training of most customers.
- Cst-20: Security budgetary constraints which limit the development of good security policies and procedures, limit the security training of personnel, and constrain the types of security tools and services to properly monitor, test, and protect the resources.
- Cst-21: Sharing of known security vulnerabilities and security incidents limited by legal and/or regulatory factors which can cause vulnerabilities to perpetuate.
- Cst-23: Lack of standards across interfaces which can lead to ad hoc engineering, difficulty in testing between vendor systems, and increased likelihood of security holes.

3.2.3.2 Specific Interface Category 1a Issues

Control systems with high data accuracy requirements and high availability, as well as media and/or compute constraints have the following characteristics:

- Typically this interface is between a SCADA system and critical field equipment, but can also be between field equipment such as protective relays
- Confidentiality – Low; Integrity – High; Availability – High
- Media is usually narrowband, limiting the volume of traffic and impacting the types of security measures that are feasible
- IEDs can be limited in compute power
- IEDs are on poletops and other insecure locations
- Wireless media is often less expensive than wired media, which mean that wireless vulnerabilities exists, and will require security controls appropriate for wireless
- None of the communication protocols currently used (primarily DNP3 and sometimes IEC 61850) are typically implemented with security measures, although IEC 62351 (which are the security standards for these protocols) is now available
- These functions have real-time operational requirements, with critical time latencies, which limits the choices for stopping or mitigating on-going attacks

- Some of the equipment is legacy (particularly the RTUs) which limit the types of security controls that could be implemented without replacing or upgrading the equipment
- Key management with thousands of devices is an issue that needs to be solved
- Since confidentiality has not been perceived as important, and where the media and compute constraints apply, encryption may not necessarily be required for general messaging

Some examples include interfaces:

- Between SCADA and transmission legacy field equipment such as Remote Terminal Units (RTUs)
- Between SCADA and legacy but critical distribution equipment such as feeder breakers and load shedding breakers

3.2.3.3 Security Control Requirements for Interface Category 1a

Using the DHS "*Catalog of Control Systems Security*" (DHS-CSC) as a checklist and assuming that the general DHS security requirements are also met, the following security requirements are considered high priority for this Interface Category:

- Physical and Environmental Security *(DHS-CSC 2.4)*
  - Physical device access authorization *(DHS-CSC 2.4.3)*
    - ➢ *Authorization for device access should include identity establishment, role-based access control, and careful maintenance of access mechanisms such as keys and passwords.*
  - Physical device access control *(DHS-CSC 2.4.4)*
    - ➢ *Locked boxes, electronic keys, and monitoring of locks for pole-top devices and other physically vulnerable equipment should be used*
- Configuration management control *(DHS-CSC 2.6)*
  - Configuration change control *(DHS-CSC 2.6.3)*
    - ➢ *Configuration management is critical for ensuring high reliability, and therefore changes should be very carefully controlled, including authorization through RBAC, testing of configuration changes for validity and unintended consequences, and the ability to "roll-back" any changes that do not meet the availability and/or other requirements.*
    - ➢ *Configurations can be physically changed and/or logically changed. Both types of changes should be controlled.*
    - ➢ *Configurations can address communication media (such as wireless configurations) as well as software configurations (such as parameter settings, database fields, and what software is in what system). Both types of configuration changes should be controlled.*

        - ➢ *Configurations can be changed temporarily to handle maintenance, repair, testing, etc. Configurations can also be changed permanently. Both types of configuration changes should be controlled.*

    - Monitoring configuration changes *(DHS-CSC 2.6.4)*

        - ➢ *Communication configurations using meshed wireless systems to connect to field equipment should have continuous monitoring to ensure configurations are still valid, not compromised, nor denying service.*

        - ➢ *Monitoring configuration changes for systems not under the control of a single organization should ensure that all "stakeholders" receive (or are permitted to receive) notification of changes.*

    - Configuration settings *(DHS-CSC 2.6.6)*

        - ➢ *Configuration settings should be restricted to meet the requirements, while still remaining flexible enough to meet unexpected requirements or emergency situations.*

- System and Communication Protection *(DHS-CSC 2.8)*

    - Denial of service protection *(DHS-CSC 2.8.5)*

        - ➢ *Although it can be difficult to protect against all denial of service attacks, Network and System Management (NSM) can provide intrusion detection and resource exhaustion detection so that mitigating actions can be rapidly invoked*

        - ➢ *IEC 62351-7 and other NSM technologies should be implemented to provide communication path monitoring to detect permanent and temporary path failures, as well as equipment and software failures*

        - ➢ *Redundancy of measurements can increase sources of data, so that denial from one source can be mitigated by access to the redundant source. Redundancy should be used where availability requirements are particularly stringent.*

        - ➢ *Redundancy of systems and equipment can increase the availability of visibility and software analysis. Redundancy, such as backup systems, backup data, or alternate analysis software, should be used where availability requirements are particularly stringent.*

        - ➢ *Wireless media can be particularly vulnerable to denial of service attacks, so mechanisms to, at a minimum, detect denial of service, and, for time-critical data, to provide alternate means to acquire this data either through redundancy or estimation, as appropriate.*

    - Resource priority *(DHS-CSC 2.8.6)*

        - ➢ *For similar time latency requirements, higher priority data should be retrieved before lower priority data*

        - ➢ *During emergencies, priority of data should be strictly enforced*

        - ➢ *No critical data should be lost due to communication failures*

    - Boundary protection *(DHS-CSC 2.8.7)*

    - *Except for SCADA systems themselves, access to SCADA data should be limited to one-way retrieval of data from a database or other site updated by the SCADA systems*
    - *Problems with one field device should not impact other field devices or SCADA monitoring of other field devices*
  - Communication integrity *(DHS-CSC 2.8.8)*
    - *IEC 62351 security standards should be used to provide communication integrity of data*
  - Cryptographic key establishment and management *(DHS-CSC 2.8.11)*
    - *Cryptography used for ensuring integrity should use key establishment and management techniques appropriate to legacy systems and communications, recognizing that direct access to certificates by field equipment is generally not feasible.*
    - *Key management for the field equipment and communication channels in this Interface Category has not been clearly developed as yet. This effort is underway in the IEC 62351 standards, and should be implemented when finalized.*
    - *"Bump-in-the-wire" technology may be used if no alternative is feasible*
  - Transmission of security parameters *(DHS-CSC 2.8.14)*
    - *IEC 62351 security standards should be used to ensure the secure transmission of security parameters*
  - Security roles *(DHS-CSC 2.8.19)*
    - *Role-Based Access Control (RBAC) should be used to establish precisely which individuals and applications play which roles, and what access authority each role has with respect to information being monitored and controlled over the interface.*
    - *Role access authorization should be per data item, not just by equipment or group of data. If legacy equipment and communication protocols do not permit this level of access control, then compensating security methods should be provided, such as limiting access within the SCADA system database.*
  - Message authenticity *(DHS-CSC 2.8.20)*
    - *IEC 62351 security standards should be used to authenticate messages*
  - Fail in known state *(DHS-CSC 2.8.24)*
    - *All equipment should revert to a previously-defined default condition upon loss of communications. This default condition should ensure minimal disruption to critical systems.*
    - *All failed equipment should not affect other equipment or disrupt critical systems.*
- Incident Response *(DHS-CSC 2.12)*
  - Continuity of operations plan *(DHS-CSC 2.12.2)*

  - ➢ *Power system operations incident planning should be extended to preparing not only for power system equipment and communications failures and overloads, but also for information infrastructure "failures" including inadvertent losses as well as deliberate attacks on information.*

  - ➢ *Critical information should be available from multiple sources if possible. If these additional sources have the information, but do not normally provide this information, then the incident plan should include methods for rapid access to these other sources. For example, meters can provide voltage information through the AMI system if normal access to DA equipment is not available.*

  - ➢ *Calculations should validate information and provide estimates for additional information*

  - ➢ *Power flow analysis of distribution systems (as well as transmission systems) should be available to provide estimated data as well as models for assessing the impact of incidents.*

  - ➢ *Control of power system and communications equipment should be included in the incident plan to allow remote actions to ameliorate the impact of incidents.*

- – Continuity of operations roles and responsibilities *(DHS-CSC 2.12.3)*

  - ➢ *Power system operations incident planning should include the clear definition of roles to be played by all involved personnel*

  - ➢ *The incident plan should include the roles for field equipment (such as default settings on loss of remote communications)*

  - ➢ *Certain software applications and systems (such as Contingency Analysis, Demand Response, DER management, Direct Load Control, and other tools) should be in the incident plan for monitoring, assessing, and controlling equipment during emergency situations.*

- – Incident response training, testing, and update *(DHS-CSC 2.12.4, .5, .6)*

  - ➢ *Incident plans that are only on paper are virtually useless. Periodic training and testing must also take place on the interfaces and equipment associated with this Interface Category – while not disrupting normal power system operations.*

- – Incident handling *(DHS-CSC 2.12.7)*

  - ➢ *During an incident, for power system operations relying on the interfaces in this Interface Category, the key will be to utilize the incident plans, but also be flexible and aware enough to respond to unexpected or unplanned for situations. This will take training, access to information from multiple sources, and the ability to try innovative approaches if the planned approach is not succeeding.*

- – Incident monitoring *(DHS-CSC 2.12.8)*

  - ➢ *Alarm and event monitoring should include not only equipment and power system events, but also security events. This A&E monitoring could be an expansion of SCADA operations*

- – Incident reporting *(DHS-CSC 2.12.8)*

- ➢ *All assessments of anomalies and/or alarms and events should be reported to the appropriate level so that any necessary correlations and corrective actions can take place*
- ➢ *Often incidents are not reported outside a small group to avoid either embarrassment or the possibility that a different attacker would learn about it and use it again. However, great care should be taken not to use the latter excuse when the real reason is the former, since corrective action by other groups with similar vulnerabilities should also take place.*

– Alternate control center *(DHS-CSC 2.12.15)*

- ➢ *Alternate control centers may be needed for transmission and distribution operational centers. The possibility for such an alternate center should be part of any design, even if not carried out in the near term.*

– Control system backup *(DHS-CSC 2.12.16)*

- ➢ *All critical operational data should be backed up, using standard methods for ensuring that bad data is not written over the good data*

– Control system recovery and reconstitution *(DHS-CSC 2.12.17)*

- ➢ *All operational systems should be designed so that authorized personnel can recover the previous state of the system after a deliberate attack or an inadvertent failure or mistake. This may include retrieving metering and other information from the customer sites as well as using backup data.*

- System and Information Integrity *(DHS-CSC 2.14)*

  – System monitoring tools and techniques *(DHS-CSC 2.14.4)*

  - ➢ *Field equipment and SCADA systems should include intrusion detection and should use their own monitoring capabilities to identify and alarm security events. If legacy equipment and communication protocols do not permit this level of event monitoring, then compensating security methods should be provided, such as additional monitoring of equipment status to detect shut-downs, restarts, and physical access.*

  – Security alerts and advisories *(DHS-CSC 2.14.5)*

  - ➢ *SCADA alarm and event handling of power system events should be extended to security alarm and events of information system events, with such alarms being directed to security personnel.*

  – Software and information integrity *(DHS-CSC 2.14.7)*

  - ➢ *Communication protocols used over these interfaces should include authentication and integrity validation, such as is specified in the IEC 62351 standards for IEC 61850, IEC 60870-5, and DNP3.*
  - ➢ *Power system operations should be extended to assessing the validity of information received from the field equipment through multiple methods, such as reasonability assessment, redundancy, power flow-based estimations, etc.*

- ➢ *For field equipment, monitoring of software changes, software halting, software restarts, etc. should be included in SCADA monitoring.*
- ➢ *Availability of key information should be monitored and alarmed if not available within the required timeframe. This availability should include field measurements, software application execution results, and personnel inputs.*

- – Information input restrictions *(DHS-CSC 2.14.9)*
  - ➢ *RBAC should be implemented to restrict input to authorized personnel and software applications.*
- – Information input accuracy, completeness, validity, and authenticity *(DHS-CSC 2.14.10)*
  - ➢ *All input, whether from authorized personnel or software applications or inputs from field sensors, should be checked as much as feasible for accuracy, completeness, validity, and authenticity.*
  - ➢ *In particular, SCADA systems and field equipment should include reasonability checks, redundancy checking, and power-flow-based assessments of information accuracy*
  - ➢ *Software patches and upgrades should be validated very extensively before being implemented, particularly for sensitive field equipment*
- – Error handling *(DHS-CSC 2.14.11)*
  - ➢ *All errors, whether associated with personnel inputs, software applications, communication errors, and/or sensor inputs, should be logged and the appropriate personnel notified*
  - ➢ *Categorization and prioritization of errors should be provided to ensure the most important errors and alarms are sent to the appropriate personnel in a timely manner.*

- Access Control *(DHS-CSC 2.15)*
  - – Access enforcement *(DHS-CSC 2.15.7)*
    - ➢ *Role-Based Access Control (RBAC) should be implemented per data item, not just by equipment or group of data. IEC 62351-8 (still under development) will specify these RBAC requirements specifically.*
    - ➢ *If legacy equipment and communication protocols do not permit this level of access control, then compensating security methods should be provided, such as limiting access within the SCADA system database.*
  - – Least privilege *(DHS-CSC 2.15.9)*
    - ➢ *Role-Based Access Control should use the concept of least privilege when designing roles and assigning individuals and applications to those roles. This is particularly important for sensitive information from field equipment.*
  - – User identification and authentication *(DHS-CSC 2.15.10)*

    - ➢ *All users and processes must be identified and their actions authenticated by role-based access control.*
  - Permitted actions without identification or authentication *(DHS-CSC 2.15.11)*
    - ➢ *Particularly for this Interface Category, it is recognized that authentication may not be implemented immediately due to legacy systems, communications, and equipment.*
    - ➢ *However, monitoring and logging of ALL control commands can be implemented "relatively" easily using existing SCADA and field equipment capabilities. Therefore, at least identification and logging of actions should be required.*
  - Passwords *(DHS-CSC 2.15.16)*
    - ➢ *Passwords, using strong authentication, should be required for all access to field equipment, and should be used in conjunction with RBAC.*
    - ➢ *Default passwords should be changed immediately upon installation of systems and equipment.*
  - Wireless access restrictions *(DHS-CSC 2.15.26)*
    - ➢ *Wireless systems have particular security vulnerabilities so that very clear guidelines should be developed to identify the types of information that can and cannot go over wireless media.*
- Audit and Accountability *(DHS-CSC 2.16)*
  - Auditable events *(DHS-CSC 2.16.2)*
    - ➢ *Power system events and all security-related events should be logged and timestamped for later analysis.*
    - ➢ *Categories and priorities of events should be established to ensure critical event information is provided to the right person or application for responding in a timely manner.*
  - Time stamps *(DHS-CSC 2.16.8)*
    - ➢ *Appropriately accurate timestamps are critical to being able to reconstruct the sequence of events, particularly across different systems and regions.*
    - ➢ *Therefore timestamp accuracy and granularity should be determined for different types of events and/or equipment.*
    - ➢ *Time synchronization should be provide for all field equipment.*

3.2.4 Interface Category 1b: Control Systems with High Data Accuracy Requirements, as well as Media and/or Compute Constraints, but Not High Availability

3.2.4.1 Interface Category 1b Characteristics

- Cst-2: High requirement for integrity and/or accuracy of data which influences not only the types of typical security measures, but also necessitates strong accuracy and error checking.
- Cst-3: High requirement for availability which influences system design, network configuration, and procedures for achieving the necessary availability
- Cst-4: Low bandwidth of communications channels which limits the types of security measures which could be employed per channel.
- Cst-5: Microprocessor constraints on memory and compute capabilities which limits the types of security measures which could be employed.
- Cst-9: Real-time operational requirements which entail short acceptable time latencies, and limit the choices for stopping or mitigating on-going attacks.
- Cst-10: Legacy end-devices and systems which limit the types, thoroughness, or effectiveness of different security measures which could be employed.
- Cst-11: Legacy communication protocols which limit the types, thoroughness, or effectiveness of different security measures which could be employed.
- Cst-12: Insecure locations which cannot be made more secure due to their physical environment or ownership.
- Cst-13: Key management for large numbers of devices which can limit the methods for deploying and revoking keys.
- Cst-14: Patch and update management constraints for sensitive devices which limits the frequency of updating security patches.
- Cst-16: Environmental and physical access constraints which limit the types of security measures, particularly physical security.
- Cst-18: Lack of security-consciousness in personnel which can cause inadvertent by-passing of security measures and can limit the number of properly trained personnel to manage and secure resources. This includes the lack of any security training of most customers.
- Cst-20: Security budgetary constraints which limit the development of good security policies and procedures, limit the security training of personnel, and constrain the types of security tools and services to properly monitor, test, and protect the resources.
- Cst-21: Sharing of known security vulnerabilities and security incidents limited by legal and/or regulatory factors which can cause vulnerabilities to perpetuate.

- Cst-23: Lack of standards across interfaces which can lead to ad hoc engineering, difficulty in testing between vendor systems, and increased likelihood of security holes.

3.2.4.2 Specific Interface Category 1b Issues

Control systems with high data accuracy requirements, as well as media and/or compute constraints, but not high availability, have the following characteristics:

- Typically this interface is between a SCADA system and non-critical field equipment, but can also be between field equipment such as automated switches on distribution feeders
- Confidentiality – Low; Integrity – High; Availability – Med
- Media is usually narrowband, limiting the volume of traffic and impacting the types of security measures that are feasible
- IEDs can be limited in compute power
- IEDs are on poletops and other insecure locations
- Wireless media is often less expensive than wired media, which mean that wireless vulnerabilities exists, and will require security controls appropriate for wireless
- None of the communication protocols currently used (primarily DNP3 and sometimes IEC 61850) are typically implemented with security measures, although IEC 62351 (which are the security standards for these protocols) is now available
- These functions have real-time operational requirements, with critical time latencies, which limits the choices for stopping or mitigating on-going attacks
- Some of the equipment is legacy (particularly the RTUs) which limit the types of security controls that could be implemented without replacing or upgrading the equipment
- Key management with thousands of devices is an issue that needs to be solved
- Since confidentiality has not been perceived as important, and where the media and compute constraints apply, encryption may not necessarily be required for general messaging

Some examples include interfaces:

- Between SCADA and non-critical distribution legacy field equipment such as voltage regulators and capacitor switches
- Between automated switches on distribution feeders which have default operational modes if communications are lost.

3.2.4.3 Security Control Requirements for Interface Category 1b

The same security requirements apply to Category 1b as for Category 1a, except that denial of service requirements are not as important.

3.2.5 Interface Category 10: Interfaces That Use the AMI Network to the Customer Site

3.2.5.1 Interface Category 10 Characteristics

- Cst-1: High requirement for confidentiality and/or privacy which necessitates or strongly influences the types of security measures required.
- Cst-4: Low bandwidth of communications channels which limits the types of security measures which could be employed per channel.
- Cst-5: Microprocessor constraints on memory and compute capabilities which limits the types of security measures which could be employed.
- Cst-6: Wireless media which can pose certain types of additional security challenges.
- Cst-7: Immature or proprietary protocols which may not be adequately tested either against inadvertent compromises or deliberate attacks.
- Cst-8: Cross-organizational interactions which limit trust and compatibility of security policies and measures, including the use of out-sourced services and leased networks.
- Cst-11: Legacy communication protocols which limit the types, thoroughness, or effectiveness of different security measures which could be employed.
- Cst-12: Insecure locations which cannot be made more secure due to their physical environment or ownership.
- Cst-13: Key management for large numbers of devices which can limit the methods for deploying and revoking keys.
- Cst-15: Unknown or rapidly changing types of interactions which complicate the decisions on the types and severity of security threats and impacts.
- Cst-16: Environmental and physical access constraints which limit the types of security measures, particularly physical security.
- Cst-17: Legal constraints limiting security measures which constrain what security could be employed, such as wiretapping of suspected hackers or blocking all 3rd party access.
- Cst-19: Negative public image or fears which can limit what functions are deployed and the types of security measures mandated or regulated.
- Cst-20: Security budgetary constraints which limit the development of good security policies and procedures, limit the security training of personnel, and constrain the types of security tools and services to properly monitor, test, and protect the resources.
- Cst-21: Sharing of known security vulnerabilities and security incidents limited by legal and/or regulatory factors which can cause vulnerabilities to perpetuate.
- Cst-22: Novel business functions with unknown ramifications from security breaches which can either lead to unwarranted, burdensome security measures or, more likely, inadequate security measures.

- Cst-23: Lack of standards across interfaces which can lead to ad hoc engineering, difficulty in testing between vendor systems, and increased likelihood of security holes.

3.2.5.2 Specific Interface Category 10 Issues

The issues for this AMI System Interface Category include the following:

- Most information from the customer must be treated as confidential.
- Integrity of data is clearly important in general, but alternate means for retrieving and/or validating it can be used.
- Availability is generally low across AMI networks since they are not designed for real-time interactions or rapid request-response requirements.
- Volume of traffic across AMI networks must be kept low to avoid denial of service situations
- Meters are constrained in their compute capabilities, primarily to keep costs down, which may limit the types and layers of security which could be applied.
- Revenue-grade meters must be certified, so that patches and upgrades require extensive testing and validation
- Meshed wireless communication networks are often used, which can present challenges related to wireless availability as well as on throughput and configurations.
- Key management of millions of meters and other equipment will pose significant challenges that have not yet been addressed as standards
- Due to the relatively new technologies used in AMI networks, communication protocols have not yet stabilized as accepted standards, nor have their capabilities been proven through rigorous testing.
- AMI networks span across organizations between utilities with corporate security requirements and customers with no or limited security capabilities or understandings.
- Utility-owned meters are in physically insecure locations that are not under utility control, limiting physical security
- Many possible future interactions across the AMI network are still being designed, or are just being speculated about, or have not yet been conceived
- Customer reactions to AMI systems and capabilities are as yet unknown, and some may fear or reject the intrusion of such “Big Brother” systems.

Some examples include interfaces:

- Between MDMS and meters
- Between LMS/DRMS and Customer EMS
- Between DMS Applications and Customer DER
- Between DMS Applications and DA Field Equipment

3.2.5.3 Security Control Requirements for Interface Category 10

Using the DHS "*Catalog of Control Systems Security*" (DHS-CSC) as a checklist and assuming that the general DHS security requirements are also met, the following security requirements are considered high priority for this Interface Category:

- Physical and Environmental Security *(DHS-CSC 2.4)*
  - Physical access control *(DHS-CSC 2.4.3)*
    - ➢ *Since meters cannot prevent access by customers and other people, very strong cryptographic technologies should be implemented for registers, databases, and other sensitive material within the meter*
    - ➢ *In particular, cryptographic keys should be stored encrypted and non-contiguously, and should never be copied into RAM.*
  - Monitoring physical access *(DHS-CSC 2.4.4)*
    - ➢ *Given the vulnerability of meters to physical access, monitoring physical access should be designed into the meter and the AMI system*
    - ➢ *Tamper detection has been a meter requirement for many years. Using this capability can also help monitor physical access.*
    - ➢ *AMI network nodes should also be monitored for physical access*
    - ➢ *Locks, limited physical access, and physical means should be used for AMI headend systems*
- Configuration Management *(DHS-CSC 2.6)*
  - Configuration change control *(DHS-CSC 2.6.3)*
    - ➢ *Configuration management is critical for ensuring high reliability, and therefore changes should be very carefully controlled, including authorization through RBAC, testing of configuration changes for validity and unintended consequences, and the ability to "roll-back" any changes that do not meet the availability and/or other requirements.*
    - ➢ *Configurations can be physically changed and/or logically changed. Both types of changes should be controlled.*
    - ➢ *Configurations can address communication media (such as wireless configurations) as well as software configurations (such as parameter settings, database fields, and what software is in what system). Both types of configuration changes should be controlled.*
    - ➢ *Configurations can be changed temporarily to handle maintenance, repair, testing, etc. Configurations can also be changed permanently. Both types of configuration changes should be controlled.*
  - Monitoring configuration changes *(DHS-CSC 2.6.4)*
    - ➢ *Both meters and AMI network nodes should be monitored for configuration changes.*

        - *In particular, the connection path between the meter and the AMI Headend should be monitored so that any changes that are outside "normal" path variations in any meshed portions of the network can be alarmed.*
        - *Inability to access a meter previously accessible should be alarmed after a "reasonable" timeframe.*
        - *Communication configurations using meshed wireless systems to connect to field equipment should have continuous monitoring to ensure configurations are still valid, not compromised, nor denying service.*
        - *Monitoring configuration changes for systems not under the control of a single organization should ensure that all "stakeholders" receive (or are permitted to receive) notification of changes.*
    - Access restrictions for configuration changes *(DHS-CSC 2.6.5)*
        - *RBAC should be used to restrict access to making configuration changes to the AMI network to authorized personnel and software applications*
    - Configuration settings *(DHS-CSC 2.6.6)*
        - *RBAC should be used to restrict access to making changes to settings and parameters of the AMI network to authorized personnel and software applications*
        - *RBAC should also be used to restrict access to making setting and parameter changes to meters*
    - Configuration for least functionality *(DHS-CSC 2.6.7)*
        - *AMI networks should not (yet) be strictly restricted to least functionality since there are expectations that they could be used for many different and unknown functions. However, some restrictions should limit obviously out-of-scope functions.*
        - *That said, new functions should be added to AMI networks with care not to unnecessarily impact the performance and security of existing functions.*
        - *Metering interfaces should be strictly limited to known metering functions*
    - Factory default authentication management *(DHS-CSC 2.6.10)*
        - *Meters should have factory-provided default certificates to secure them during shipment. These certificates should be changed to utility-provided certificates upon arrival and warehousing. Another certificate change should occur when installed in the field.*
        - *AMI network components, including the AMI headend should also have their factory-provided default certificates and/or passwords changed immediately upon installation.*
- System and Communication Protection *(DHS-CSC 2.8)*
    - Security function isolation *(DHS-CSC 2.8.3)*
        - *Many "security functions" are actually part of the normal AMI network and system management in which AMI nodes, communications, and end devices are*

monitored for anomalous events, and actions taken to mitigate problems, whether deliberately or inadvertently caused. Therefore, these security functions should not be isolated from normal operations.

  - ➢ *Some security functions, such as establishing access controls, key management, and information prioritization and flow control, should be separated from operational functions.*

- – Denial of service protection *(DHS-CSC 2.8.5)*
  - ➢ *Although availability security requirements should not be high for any individual interaction across an AMI system, the overall availability of the AMI should be relatively high. Therefore, any critical AMI component, such as the AMI headend or backbone communications, should be designed with redundancy and/or other configurations to enhance availability.*
  - ➢ *Where availability requirements are more important, the AMI system could provide redundancy of equipment, alternate paths, battery backup, and other methods for improving availability.*
  - ➢ *Network and System Management (NSM) should provide intrusion detection and resource exhaustion detection, with notification of these events securely provided to appropriate personnel and/or systems.*
  - ➢ *IEC 62351-7 and other NSM technologies should be implemented on the AMI networks to provide communication path monitoring to detect permanent and temporary path failures, as well as equipment and software failures*
  - ➢ *Redundancy of measurements, where these are available, can increase sources of data and thus minimize the impact of denial-of-service events. Although not generally feasible for individual metering, redundant measurements for distribution system monitoring could be provided.*
  - ➢ *Wireless media are particularly vulnerable to denial of service attacks, so mechanisms should be provided to, at a minimum, detect denial of service, and, for time-critical data, to provide alternate means to acquire this data either through redundancy or estimation, as appropriate.*
- – Resource priority *(DHS-CSC 2.8.6)*
  - ➢ *Priority of different types of data should be clearly defined and implemented on AMI systems*
  - ➢ *For similar time latency requirements, higher priority data should be retrieved before lower priority data*
  - ➢ *During emergencies, priority of data should be strictly enforced, including the rejection of all low priority data*
  - ➢ *No critical data should be lost due to communication failures, so that it can be retrieved at a later time with no loss of accuracy.*
- – Boundary protection *(DHS-CSC 2.8.7)*

  - ➢ *AMI system boundaries should be clearly defined, including at least separate boundaries for metering information, for power system operational information, for security management information, for sensitive customer information, and for non-utility "public" information*

  - ➢ *These AMI system boundaries should be protected as appropriate and as feasible through physical separation, virtual separation, layered security, RBAC, and/or other security mechanisms.*

  - ➢ *Information traffic across these boundaries should be avoided*

  - ➢ *Any cross-boundary interactions should be monitored and logged, with unexpected interactions causing alarms*

  - ➢ *Access to data transmitted across the AMI system should be limited to authorized systems through RBAC procedures as much as feasible, recognizing that field locations of AMI components must be considered untrusted*

  - ➢ *Information from the Home Area Network (HAN) should always be treated as untrusted, with strict constraints imposed on what types of data can be exchanged between the HAN and the AMI system. Unnecessary interactions should be avoided.*

  - ➢ *Security problems within one area of the AMI system should not impact other areas of the AMI system*

  - ➢ *Information crossing any boundary should be validated for reasonability, expected accuracy, and possible modification, with anomalies timestamped and logged, and/or alarmed.*

- – Communication integrity *(DHS-CSC 2.8.8)*

  - ➢ *For information with high integrity requirements, authentication of the source of the information should be used. This authentication may or may not require encryption of the information.*

  - ➢ *All information transmitted across an AMI system should be validated to the appropriate level of accuracy, using VEE practices where appropriate or other similar reasonability and validity checking methods.*

  - ➢ *Given the untrusted nature of the AMI system, critical information should always have backup or redundant means of access, including alternate communication paths (e.g. truck-roll), alternate sources (e.g. secondary voltage sources), or methods for estimation (e.g. VEE or State Estimation function).*

- – Communication confidentiality *(DHS-CSC 2.8.9)*

  - ➢ *For information with high confidentiality requirements, cryptographic mechanisms should be used, as defined in appropriate AMI security standards*

  - ➢ *The AMI system and its components should be designed to handle the additional compute and communication traffic requirements to utilize the recommended cryptographic technologies.*

- – Trusted path *(DHS-CSC 2.8.10)*

  - ➢ *Since AMI systems cannot provide completely trusted paths nor independent certificate management for field devices, in addition to establishing best practices for such paths, all information should be validated and checked for confidentiality compromises, and certain sensitive data should checked periodically against alternate sources of this data.*

- – Cryptographic key establishment and management *(DHS-CSC 2.8.11)*
  - ➢ *Cryptography used for sensitive information should use key establishment and management techniques appropriate to meters, field equipment, and bandwidth-limited communications, recognizing that direct access to certificates by field equipment is generally not feasible.*
  - ➢ *Key management for large numbers of field equipment and bandwidth-limited communication channels has not been developed as yet. This effort is underway in the IEC 62351 standards, and should be implemented when finalized.*
  - ➢ *"Bump-in-the-wire" technology could be used where feasible*
- – Transmission of security parameters *(DHS-CSC 2.8.14)*
  - ➢ *Security standards for AMI systems, when available, should be used to ensure the secure transmission of security parameters. These could include the ANSI C12.22, and IEC standards*
- – Security roles *(DHS-CSC 2.8.19)*
  - ➢ *Role-Based Access Control (RBAC) should be used to establish precisely which individuals and applications play which roles, and what access authority each role has with respect to information being monitored and controlled over the interface.*
  - ➢ *Role access authorization should be per data item, not just by equipment or group of data.*
  - ➢ *If legacy equipment and/or bandwidth-limited communication protocols do not permit per data item access control, then compensating security methods should be provided at the enterprise level to limit access to data items in databases.*
- – Message authenticity *(DHS-CSC 2.8.20)*
  - ➢ *IEC 62351 security standards should be used to authenticate messages*
- – Fail in known state *(DHS-CSC 2.8.24)*
  - ➢ *All equipment should revert to a previously-defined default condition upon loss of communications. This default condition should ensure minimal disruption to critical systems*
  - ➢ *All failed equipment should not affect other equipment or disrupt critical systems.*
- – Confidentiality of information at rest *(DHS-CSC 2.8.28)*
  - ➢ *AMI system components will contain information that must remain confidential and/or private. These components should use cryptographic techniques to ensure the confidentiality of this information.*

- Incident Response *(DHS-CSC 2.12)*
  - Continuity of operations plan *(DHS-CSC 2.12.2)*
    - *Critical information should be available from multiple sources if possible. If these additional sources have the information, but do not normally provide this information, then the incident plan should include methods for rapid access to these other sources. For example, meters can provide voltage information through the AMI system if normal access to DA equipment is not available.*
  - Continuity of operations roles and responsibilities *(DHS-CSC 2.12.3)*
    - *AMI system incident planning should include the clear definition of roles to be played by all involved personnel*
    - *The incident plan should include the roles for field equipment upon the occurrence of an incident. For instance, all equipment should have default settings or modes in case of the loss of communications beyond expected limits.*
    - *Certain software applications and systems (such as tamper detection, revenue protection, confidentiality monitoring, and other tools) should be included the incident plan for monitoring, assessing, and controlling equipment during emergency situations.*
  - Incident response training, testing, and update *(DHS-CSC 2.12.4, .5, .6)*
    - *Incident plans that are only on paper are virtually useless. Periodic training and testing must also take place on the interfaces and equipment associated with this Interface Category – while not disrupting normal power system operations or compromising metering confidentiality.*
    - *Power system training simulators and testing tools can help train personnel in handling security-related incidents*
  - Incident handling *(DHS-CSC 2.12.7)*
    - *Unlike some other systems, control systems cannot just be shut down during an incident – they must be kept running.*
    - *During an incident, the key will be to utilize the incident plans, but also be flexible and aware enough to respond to unexpected or unplanned for situations. This will take training, access to information from multiple sources, and the ability to try innovative approaches if the planned approach is not succeeding.*
    - *AMI systems, if used to send demand response or other signals to customer-based DER equipment, should be designed to expect equipment and system failures, so that critical DER equipment can continue to perform as needed to help maintain power system reliability.*
  - Incident monitoring *(DHS-CSC 2.12.8)*
    - *All anomalies should be monitored and assessed, both automatically, and if warranted, brought to the attention of a security operator. Sometimes what appears to be innocuous to a power system operator or customer representative could be a critical signal of a possible security attack to a security operator*

        - ➢ *Alarm and event monitoring of systems and equipment connected to the AMI system should include not only equipment and power system events, but also security events. This A&E monitoring could be an expansion of AMI system management.*
        - ➢ *All alarm and events should be assessed for security-related concerns as well as power system operational concerns or customer-related concerns.*
        - ➢ *Alarm and event logs should contain a synchronized timestamp that is appropriately accurate so that correlations across wide spread systems can take place*
        - ➢ *For some types of critical situations, the state and measurements of the power system and/or the information system should be captured and saved periodically (every 2-10 seconds for critical power system states), then discarded after a while if no incident occurs. If an incident does occur, then the sequence of periodic saved information can be critical to understanding what happened.*
    - Incident reporting *(DHS-CSC 2.12.9)*
        - ➢ *All assessments of anomalies and/or alarms and events should be reported to the appropriate level so that any necessary correlations and corrective actions can take place*
        - ➢ *Often incidents are not reported outside a small group to avoid either embarrassment or the possibility that a different attacker would learn about it and use it again. However, great care should be taken not to use the latter excuse when the real reason is the former, since corrective action by other groups with similar vulnerabilities should also take place.*
    - Alternate control center *(DHS-CSC 2.12.15)*
        - ➢ *Alternate control centers may be needed by AMI systems as their functionality and criticality grow. The possibility for such an alternate center should be part of any design, even if not carried out in the near term.*
    - Control system backup *(DHS-CSC 2.12.16)*
        - ➢ *All AMI system data should be backed up, using standard methods for ensuring that bad data is not written over the good data*
    - Control system recovery and reconstitution *(DHS-CSC 2.12.17)*
        - ➢ *All AMI systems should be designed so that authorized personnel can recover the previous state of the system after a deliberate attack or an inadvertent failure or mistake. This may include retrieving metering and other information from the customer sites as well as using backup data.*
- System and Information Integrity *(DHS-CSC 2.14)*
    - System monitoring tools and techniques *(DHS-CSC 2.14.4)*
        - ➢ *AMI systems should include intrusion detection for all components, including meters, network nodes, and the AMI headend. Intrusions should be reported using the AMI system monitoring capabilities to identify and alarm security events.*

    - *If communication and equipment constraints do not permit this level of event monitoring, then compensating security methods should be provided, such as additional monitoring of equipment status to detect shut-downs, restarts, and physical access.*

- Security alerts and advisories *(DHS-CSC 2.14.5)*
    - *AMI system alarm and event handling of events should be extended to security alarm and events of information system events, with such alarms being directed to security personnel.*
- Software and information integrity *(DHS-CSC 2.14.7)*
    - *Communication protocols used over the AMI system should include authentication and integrity validation.*
    - *AMI systems should assess the validity of information received from the field equipment through multiple methods, such as reasonability assessment, redundancy, power flow-based estimations, etc.*
    - *AMI systems that monitor field equipment should also monitor software changes, software halting, software restarts, etc.*
    - *Availability of key information should be monitored and alarmed if not available within the required timeframe. This availability should include field measurements, software application execution results, and personnel inputs.*
- Information input restrictions *(DHS-CSC 2.14.9)*
    - *RBAC should be implemented to restrict input to authorized personnel and software applications.*
    - *All information received from field locations should be strictly limited to authorized personnel, potentially with two-step authentication for critical interactions.*
- Information input accuracy, completeness, validity, and authenticity *(DHS-CSC 2.14.10)*
    - *All input, whether from authorized personnel or software applications or inputs from field sensors, should be checked as much as feasible for accuracy, completeness, validity, and authenticity.*
    - *In particular, AMI systems should include reasonability checks, redundancy checking, and revenue protection assessments of information accuracy*
    - *Software patches and upgrades should be validated very extensively before being implemented, particularly for sensitive field equipment*
- Error handling *(DHS-CSC 2.14.11)*
    - *All errors, whether associated with personnel inputs, software applications, communication errors, and/or sensor inputs, should be logged and the appropriate personnel notified*

    - ➢ *Categorization and prioritization of errors should be provided to ensure the most important errors and alarms are sent to the appropriate personnel in a timely manner.*

- Access Control *(DHS-CSC 2.15)*
  - Access enforcement *(DHS-CSC 2.15.7)*
    - ➢ *Role-Based Access Control (RBAC) should be implemented per data item, not just by equipment or group of data.*
    - ➢ *If legacy equipment and communication constraints do not permit this level of access control, then compensating security methods should be provided, such as limiting access within the AMI system database.*
  - Least privilege *(DHS-CSC 2.15.9)*
    - ➢ *Role-Based Access Control should use the concept of least privilege when designing roles and assigning individuals and applications to those roles. This is particularly important for sensitive information from field equipment.*
  - User identification or authentication *(DHS-CSC 2.15.10)*
    - ➢ *All users and processes must be identified and their actions authenticated by role-based access control.*
  - Permitted actions without identification or authentication *(DHS-CSC 2.15.11)*
    - ➢ *Monitoring and logging of ALL control commands should be implemented, even during emergency overrides. Therefore, at least identification and logging of actions should be required.*
  - Passwords *(DHS-CSC 2.15.16)*
    - ➢ *Passwords, using strong authentication, should be required for all access AMI components, and should be used in conjunction with RBAC.*
    - ➢ *Default passwords should be changed immediately upon installation of systems and equipment.*
  - Wireless access restrictions *(DHS-CSC 2.15.26)*
    - ➢ *Wireless systems have particular security vulnerabilities so that very clear guidelines should be developed to identify the security measures to be implemented and the types of information that are permitted and not permitted to go over wireless media.*
- Audit and Accountability *(DHS-CSC 2.16)*
  - Auditable events *(DHS-CSC 2.16.2)*
    - ➢ *Power system events, customer-based events, and all security-related events should be logged and timestamped for later analysis.*
    - ➢ *Categories and priorities of events should be established to ensure critical event information is provided to the right person or application for responding in a timely manner.*

- Time stamps *(DHS-CSC 2.16.8)*
    - *Appropriately accurate timestamps are critical to being able to reconstruct the sequence of events, particularly across different systems and regions.*
    - *Therefore timestamp accuracy and granularity should be determined for different types of events and/or equipment.*
    - *Time synchronization should be provide for all field equipment.*
- Audit generation *(DHS-CSC 2.16.15)*
- Non-Repudiation *(DHS-CSC 2.16.16)*

3.2.6 Interface Category 14: Metering Interfaces

3.2.6.1 Interface Category 14 Characteristics

- Cst-1: High requirement for confidentiality and/or privacy which necessitates or strongly influences the types of security measures required.
- Cst-2: High requirement for integrity and/or accuracy of data which influences not only the types of typical security measures, but also necessitates strong accuracy and error checking.
- Cst-4: Low bandwidth of communications channels which limits the types of security measures which could be employed per channel.
- Cst-5: Microprocessor constraints on memory and compute capabilities which limits the types of security measures which could be employed.
- Cst-6: Wireless media which can pose certain types of additional security challenges.
- Cst-7: Immature or proprietary protocols which may not be adequately tested either against inadvertent compromises or deliberate attacks.
- Cst-8: Cross-organizational interactions which limit trust and compatibility of security policies and measures, including the use of out-sourced services and leased networks.
- Cst-10: Legacy end-devices and systems which limit the types, thoroughness, or effectiveness of different security measures which could be employed.
- Cst-11: Legacy communication protocols which limit the types, thoroughness, or effectiveness of different security measures which could be employed.
- Cst-12: Insecure locations which cannot be made more secure due to their physical environment or ownership.
- Cst-13: Key management for large numbers of devices which can limit the methods for deploying and revoking keys.
- Cst-14: Patch and update management constraints for sensitive devices which limits the frequency of updating security patches.

- Cst-16: Environmental and physical access constraints which limit the types of security measures, particularly physical security.
- Cst-17: Legal constraints limiting security measures which constrain what security could be employed, such as wiretapping of suspected hackers or blocking all 3rd party access.
- Cst-18: Lack of security-consciousness in personnel which can cause inadvertent by-passing of security measures and can limit the number of properly trained personnel to manage and secure resources. This includes the lack of any security training of most customers.
- Cst-19: Negative public image or fears which can limit what functions are deployed and the types of security measures mandated or regulated.
- Cst-20: Security budgetary constraints which limit the development of good security policies and procedures, limit the security training of personnel, and constrain the types of security tools and services to properly monitor, test, and protect the resources.
- Cst-23: Lack of standards across interfaces which can lead to ad hoc engineering, difficulty in testing between vendor systems, and increased likelihood of security holes.

3.2.6.2 Specific Interface Category 14 Issues

The issues for this Metering Interface Category include the following:

- Most metering information from the customer must be treated as confidential since profiles of hourly energy usage (as opposed to monthly energy usage) could be used for unauthorized and/or illegal activities.
- Integrity of revenue-grade metering data is vital since it has a direct financial impact on all stakeholders of the loads and generation being metered.
- Availability of metering data is important but not critical, since alternate means for retrieving metering data can still be used.
- Meters are constrained in their compute capabilities, primarily to keep costs down, which may limit the types and layers of security which could be applied.
- Revenue-grade meters must be certified, so that patches and upgrades require extensive testing and validation
- Key management of millions of meters will pose significant challenges that have not yet been addressed as standards
- Due to the relatively new technologies used with smart meters, some standards have not been fully developed, nor have their capabilities been proven through rigorous testing.
- Multiple (authorized) stakeholders, including customers, utilities, and third parties, may need access to energy usage either directly from the meter or after it has been processed and validated for settlements and billing, thus adding cross-organizational security concerns.

- Utility-owned meters are in physically insecure locations that are not under utility control, limiting physical security
- Customer reactions to AMI systems and smart meters are as yet unknown, and some may fear or reject the intrusion of such "Big Brother" systems.

Some examples include interfaces:

- Between MDMS and meters (via the AMI headend)
- Between customer EMS and meters
- Between field crew tools and meters
- Between meters and sub-meters
- Between customer DER and sub-meters
- Between electric vehicles and sub-meters

3.2.6.3 Security Control Requirements for Interface Category 14

Using the DHS "*Catalog of Control Systems Security*" (DHS-CSC) as a checklist and assuming that the general DHS security requirements are also met, the following security requirements are considered high priority for this Interface Category:

- Physical and Environmental Security *(DHS-CSC 2.4)*
  - Physical access control *(DHS-CSC 2.4.3)*
    - ➢ *Since meters cannot prevent access by customers and other people, very strong cryptographic technologies should be implemented for registers, databases, and other sensitive material within the meter*
    - ➢ *In particular, cryptographic keys should be stored encrypted and non-contiguously, and should never be copied into RAM.*
  - Monitoring physical access *(DHS-CSC 2.4.4)*
    - ➢ *Given the vulnerability of meters to physical access, monitoring physical access should be designed into the meter and any of its interfaces with metered equipment*
    - ➢ *Tamper detection has been a meter requirement for many years. Using this capability can also help monitor physical access.*
    - ➢ *Locks, limited physical access, and physical protection should be used for the interface between the equipment being metered and the meter*
- Configuration Management *(DHS-CSC 2.6)*
  - Configuration change control *(DHS-CSC 2.6.3)*
    - ➢ *Configuration management of metering equipment is critical for ensuring high integrity, and therefore changes should be very carefully controlled, including authorization through RBAC, testing of configuration changes for validity and*

unintended consequences, and the ability to "roll-back" any changes that do not meet the availability and/or other requirements.

    - ➢ *Configurations can be physically changed and/or logically changed. Both types of changes should be controlled.*
    - ➢ *Configurations can be changed temporarily to handle maintenance, repair, testing, etc. Configurations can also be changed permanently. Both types of configuration changes should be controlled.*
    - ➢ *All configuration changes should be timestamped and logged, with the entity making the changes identified, as well as the type of configuration changes clearly described*
  - – Monitoring configuration changes *(DHS-CSC 2.6.4)*
    - ➢ *Meters and sub-meters should be monitored for configuration changes.*
    - ➢ *In particular, the connection path between the meter and any sub-meters should be monitored so that any changes that are outside "normal" path, such as variations in any meshed portions of the network, can be alarmed.*
    - ➢ *Inability to access a meter or sub-meter previously accessible should be alarmed after a "reasonable" timeframe.*
    - ➢ *Monitoring configuration changes for systems not under the control of a single organization should ensure that all "stakeholders" receive (or are permitted to receive) notification of changes.*
  - – Access restrictions for configuration changes *(DHS-CSC 2.6.5)*
    - ➢ *RBAC should be used to restrict access to making configuration changes to the metering equipment to authorized personnel and software applications*
  - – Configuration settings *(DHS-CSC 2.6.6)*
    - ➢ *RBAC should be used to restrict access to making changes to settings and parameters of the metering equipment to authorized personnel and software applications*
  - – Configuration for least functionality *(DHS-CSC 2.6.7)*
    - ➢ *Metering equipment should be strictly limited to known metering functions*
  - – Factory default authentication management *(DHS-CSC 2.6.10)*
    - ➢ *Meters should have factory-provided default certificates to secure them during shipment. These certificates should be changed to utility-provided certificates upon arrival and warehousing. Another certificate change should occur when installed in the field.*
- System and Communication Protection *(DHS-CSC 2.8)*
  - – Security function isolation *(DHS-CSC 2.8.3)*
    - ➢ *Many "security functions" are actually part of the normal metering procedures where they are monitored for anomalous events, and actions taken to mitigate*

problems, whether deliberately or inadvertently caused. Therefore, these security functions should not be isolated from normal operations.

  - ➢ *Some security functions, such as establishing access controls, key management, and information prioritization and flow control, should be separated from metrology functions.*

- – Denial of service protection *(DHS-CSC 2.8.5)*

  - ➢ *For some metering, availability requirements are significant. In those cases, redundancy of equipment, alternate paths, battery backup, and other methods should be provided for improving availability.*

  - ➢ *For metering with less stringent availability requirements, alternate methods for retrieving metering information can be used, such as on-site meter reading, estimated readings, etc.*

  - ➢ *Network and System Management (NSM) should provide intrusion detection and resource exhaustion detection for metering systems, with notification of these events securely provided to appropriate personnel and/or systems.*

  - ➢ *Wireless media can be particularly vulnerable to denial of service attacks if not properly configured, so mechanisms should be provided to, at a minimum, detect denial of service, and, for time-critical data, to provide alternate means to acquire this data either through redundancy or estimation, as appropriate.*

- – Resource priority *(DHS-CSC 2.8.6)*

  - ➢ *Priority of different types of metering data should be clearly defined and identified to systems requiring access to the data. This includes priority handling of outage detection, priority identification of metering data needed for critical distribution functions, and metering data for critical locations such as first responders.*

  - ➢ *For similar time latency requirements, higher priority data should be retrieved before lower priority data*

  - ➢ *During emergencies, priority of data retrieval should be strictly enforced, including the rejection of all low priority data*

  - ➢ *No critical metering data should be lost or overwritten due to communication failures or low priority, so that it can be retrieved at a later time with no loss of accuracy.*

- – Boundary protection *(DHS-CSC 2.8.7)*

  - ➢ *Metering boundaries should be clearly defined, including separate boundaries for metrology information, for security management information, for sensitive customer information, and for non-utility "public" information.*

  - ➢ *These metering boundaries should be protected as appropriate and as feasible through physical separation, virtual separation, layered security, RBAC, and/or other security mechanisms.*

  - *Metering information crossing any boundary should be validated for reasonability, expected accuracy, and possible modification, with anomalies timestamped and logged, and/or alarmed.*
  - *Information traffic across these boundaries should be avoided*
  - *Any cross-boundary interactions should be monitored and logged, with unexpected interactions causing alarms*
  - *Security problems within another area of the AMI system should not impact metering equipment.*
- Communication integrity *(DHS-CSC 2.8.8)*
  - *Revenue metering information has high integrity requirements, so authentication of the meter should be used. This authentication may or may not require encryption of the information.*
  - *All metering information transmitted across an AMI system should be validated to the appropriate level of accuracy, using VEE practices where appropriate or other similar reasonability and validity checking methods.*
  - *Given the untrusted nature of the AMI system, critical metering information should always have backup or redundant means of access, including alternate communication paths (e.g. truck-roll), alternate sources (e.g. secondary voltage sources), or methods for estimation (e.g. VEE or State Estimation function).*
- Communication confidentiality *(DHS-CSC 2.8.9)*
  - *Most smart metering information should be considered confidential, since hourly energy usage information can be used for unauthorized or illegal activities, such as unauthorized targeting of customers for marketing purposes, or burglary if the customer site appears empty due to low energy usage.*
  - *For metering information with high confidentiality requirements, cryptographic mechanisms should be used.*
  - *The AMI system and its components should be designed to handle the additional compute and communication traffic requirements to utilize the recommended cryptographic technologies.*
- Trusted path *(DHS-CSC 2.8.10)*
  - *Since metering equipment is located at untrusted sites, no completely trusted paths exist even between meters and sub-meters. Therefore, all metering information should be validated and checked for confidentiality compromises, and certain sensitive data should checked periodically against alternate sources of this data.*
- Cryptographic key establishment and management *(DHS-CSC 2.8.11)*
  - *Cryptographic techniques used for sensitive metering information should use key establishment and management techniques appropriate to the constraints posed by millions of meters, meter compute-constraints, and bandwidth-limited*

communications, while recognizing that direct access to certificates by meters is generally not feasible.

  - ➢ *Key management for large numbers of meters and bandwidth-limited communication channels has not been developed as yet. This effort is underway in the IEC 62351 standards, and should be implemented when finalized.*

  - ➢ *"Bump-in-the-wire" security technology should not be used with meters given the lack of trust between the meter and any external equipment*

- – Transmission of security parameters *(DHS-CSC 2.8.14)*

  - ➢ *Security standards for meters, when available, should be used to ensure the secure transmission of security parameters. These could include the ANSI C12.22, and IEC standards*

- – Security roles *(DHS-CSC 2.8.19)*

  - ➢ *Role-Based Access Control (RBAC) should be used to establish precisely which individuals and applications play which roles, and what access authority each role has with respect to information being monitored and controlled over the interface.*

  - ➢ *Role access authorization should be per data item, not just by equipment or group of data.*

  - ➢ *If legacy equipment and/or bandwidth-limited communication protocols do not permit per data item access control, then compensating security methods should be provided at the enterprise level to limit access to data items in databases.*

- – Message authenticity *(DHS-CSC 2.8.20)*

  - ➢ *ANSI C12.22, IEC 62351, and/or other IEC security standards should be used to authenticate messages*

- – Fail in known state *(DHS-CSC 2.8.24)*

  - ➢ *All failed metering equipment should not affect other equipment or disrupt critical systems.*

- – Confidentiality of information at rest *(DHS-CSC 2.8.28)*

  - ➢ *Metering equipment contains information within the meter that must remain confidential and/or private. This equipment should use cryptographic techniques to ensure the confidentiality of this information, such as database encryption.*

- Incident Response *(DHS-CSC 2.12)*

  - – Continuity of operations plan *(DHS-CSC 2.12.2)*

    - ➢ *Meters can provide information that could be used for power system operations during emergency situations, so the incident plan should include methods for accessing this critical information.*

  - – Continuity of operations roles and responsibilities *(DHS-CSC 2.12.3)*

  - *Metering incident planning should include the clear definition of roles to be played by all involved personnel*
  - *Certain software applications and systems (such as tamper detection, revenue protection, confidentiality monitoring, and other tools) should be included the incident plan for monitoring, assessing, and controlling metering equipment during emergency situations.*
- Incident response training, testing, and update *(DHS-CSC 2.12.4, .5, .6)*
  - *Incident plans that are only on paper are virtually useless. Periodic training and testing must also take place on the interfaces and equipment associated with this Interface Category – while not compromising metering confidentiality.*
  - *Power system training simulators and testing tools could be expanded to use information from metering to help train personnel in handling security-related incidents.*
- Incident handling *(DHS-CSC 2.12.7)*
  - *Unlike some other systems, control systems cannot just be shut down during an incident – they must be kept running. Metering may play an increasingly large role during incidents as providing redundant sources of potentially critical information.*
  - *During an incident, the key will be to utilize the incident plans, but also be flexible and aware enough to respond to unexpected or unplanned for situations. This will take training, access to information from multiple sources, and the ability to try innovative approaches if the planned approach is not succeeding.*
- Incident monitoring *(DHS-CSC 2.12.8)*
  - *All anomalies should be monitored and assessed, both automatically, and if warranted, brought to the attention of a security operator. Sometimes what appears to be innocuous to a power system operator or customer representative could be a critical signal of a possible security attack to a security operator*
  - *Alarm and event monitoring of metering equipment should include not only metering alarms and events, but also security alarms and events. This A&E monitoring could be an expansion of AMI system metering management.*
  - *All alarm and events should be assessed for security-related concerns as well as power system operational concerns or customer-related concerns.*
  - *Alarm and event logs should contain a synchronized timestamp that is appropriately accurate so that correlations across wide spread systems can take place*
  - *For some types of critical situations, the state and measurements of the power system and/or the information system should be captured and saved periodically (every 2-10 seconds for critical power system states), then discarded after a while if no incident occurs. If an incident does occur, then the sequence of periodic saved information can be critical to understanding what happened.*

- Incident reporting *(DHS-CSC 2.12.9)*
  - ➢ *All assessments of metering anomalies and/or alarms and events should be reported to the appropriate level so that any necessary correlations and corrective actions can take place*
  - ➢ *Often incidents are not reported outside a small group to avoid either embarrassment or the possibility that a different attacker would learn about it and use it again. However, great care should be taken not to use the latter excuse when the real reason is the former, since corrective action by other groups with similar vulnerabilities should also take place.*
- Alternate control center *(DHS-CSC 2.12.15)*
  - ➢ *Alternate control centers may be needed by AMI systems as their functionality and criticality grow, including providing redundant operational data from metering equipment. The possibility for such an alternate center should be part of any design, even if not carried out in the near term.*
- Control system backup *(DHS-CSC 2.12.16)*
  - ➢ *All metering data should be backed up, using standard methods for ensuring that bad data is not written over the good data*
- Control system recovery and reconstitution *(DHS-CSC 2.12.17)*
  - ➢ *All metering systems should be designed so that authorized personnel can recover the previous state of the system after a deliberate attack or an inadvertent failure or mistake. This may include retrieving metering and other information by personnel physically visiting customer sites as well as using backup data.*

- System and Information Integrity *(DHS-CSC 2.14)*
  - System monitoring tools and techniques *(DHS-CSC 2.14.4)*
    - ➢ *Metering equipment should include intrusion detection for all components. Intrusions should be reported using the AMI system monitoring capabilities to identify and alarm security events.*
    - ➢ *If communication and equipment constraints do not permit this level of event monitoring, then compensating security methods should be provided, such as additional monitoring of equipment status to detect shut-downs, restarts, and physical access.*
  - Security alerts and advisories *(DHS-CSC 2.14.5)*
    - ➢ *Metering alarm and event handling of events should be extended to security alarm and events of information system events, with such alarms being directed to security personnel.*
  - Software and information integrity *(DHS-CSC 2.14.7)*
    - ➢ *All metering software and data should include authentication and integrity validation.*

        - ➢ *The validity of metered data should be assessed through multiple methods, such as revenue protection schemes, reasonability assessment, redundancy, estimations, etc.*
        - ➢ *Metering equipment should also log and alarm all software changes, software halting, software restarts, etc.*
        - ➢ *Availability of important information should be monitored and alarmed if not available within the required timeframe. This availability should include metering measurements, software application execution results, and personnel inputs.*
    - – Information input restrictions *(DHS-CSC 2.14.9)*
        - ➢ *RBAC should be implemented to restrict input to authorized personnel and software applications.*
        - ➢ *All information received from field locations should be strictly limited to authorized personnel, potentially with two-step authentication for critical interactions.*
    - – Information input accuracy, completeness, validity, and authenticity *(DHS-CSC 2.14.10)*
        - ➢ *All input, whether from authorized personnel or software applications or inputs from field sensors, should be checked as much as feasible for accuracy, completeness, validity, and authenticity.*
        - ➢ *Software patches and upgrades should be validated very extensively before being implemented on revenue grade metering equipment.*
    - – Error handling *(DHS-CSC 2.14.11)*
        - ➢ *All errors, whether associated with personnel inputs, software applications, communication errors, and/or sensor inputs, should be logged and the appropriate personnel notified*
        - ➢ *Categorization and prioritization of errors should be provided to ensure the most important errors and alarms are sent to the appropriate personnel in a timely manner.*
- Access Control *(DHS-CSC 2.15)*
    - – Access enforcement *(DHS-CSC 2.15.7)*
        - ➢ *Role-Based Access Control (RBAC) should be implemented per data item, not just by equipment or group of data.*
        - ➢ *If legacy equipment and communication constraints do not permit this level of access control, then compensating security methods should be provided, such as limiting access within the metering database.*
    - – Least privilege *(DHS-CSC 2.15.9)*
        - ➢ *Role-Based Access Control should use the concept of least privilege when designing roles and assigning individuals and applications to those roles. This is particularly important for sensitive information from metering equipment.*

  - Permitted actions without identification or authentication *(DHS-CSC 2.15.11)*
    - ➢ *Monitoring and logging of ALL control commands should be implemented, even during emergency overrides. Therefore, at least identification and logging of actions should be required.*
  - Passwords *(DHS-CSC 2.15.16)*
    - ➢ *Passwords, using strong authentication, should be required for all access to metering equipment, and should be used in conjunction with RBAC.*
    - ➢ *Default passwords should be changed immediately upon installation of systems metering equipment.*
  - Wireless access restrictions *(DHS-CSC 2.15.26)*
    - ➢ *Wireless systems have particular security vulnerabilities so that very clear guidelines should be developed to identify the security measures to be implemented and the types of information that are permitted and not permitted to go over wireless media.*
- Audit and Accountability *(DHS-CSC 2.16)*
  - Auditable events *(DHS-CSC 2.16.2)*
    - ➢ *Metrology events, power system events, customer-based events, and all security-related events should be logged and timestamped in the metering equipment for later analysis.*
    - ➢ *Categories and priorities of events should be established to ensure critical event information is provided to the right person or application for responding in a timely manner.*
  - Time stamps *(DHS-CSC 2.16.8)*
    - ➢ *Appropriately accurate timestamps are critical to being able to reconstruct the sequence of events, so timestamp accuracy and granularity should be determined for metering equipment.*
    - ➢ *Time synchronization should be provide for all field equipment.*

4. Use of Existing and/or Expanded Power System Management Capabilities for Security Management

One of the key issues for utilities is how to balance power system reliability, their core business requirement, with the growing need for physical and cyber security. **One of the most powerful security solutions is to utilize and expand existing power system management technologies to provide security measures.** After all, these power system management technologies (e.g. SCADA systems, Energy Management Systems, Contingency Analysis applications, Fault Location, Isolation, and Restoration capabilities) have been developed to address inadvertent security threats such as equipment failures. In addition, customer services and metering management have long focused on "revenue protection", albeit at a meter-by-meter approach. But the same (and expanded) techniques could be used to help manage the security of "smart meters". So many existing functions can be used to help address deliberate security threats as well.

4.1 Use of Power System Management Applications for Protection Against Certain Cyber Attacks

Transmission systems have long been monitored and controlled via SCADA systems with an increasing visibility into their real-time status and with increasing use of sophisticated applications to view into the less visible portions (state estimation and power flow-based applications) and assess potential future problems (load forecasts and contingency analysis). This visibility is now being expanded into broader situational awareness through wide-area measurements systems. The visibility into transmission system real-time status can also provide visibility into any inadvertent or deliberate cyber security attacks that affect transmission power system operations.

However, distribution systems are still mostly treated as static systems, needing minimal visibility to manage them. This is changing as distributed energy resources are added to feeders and installed at customer sites, and as power system reliability and efficiency become more important to regulators and customers. Distribution power flow-based applications, similar to those used for transmission systems, could provide the increased visibility needed for future power system operations. But in addition, they could form one of the most powerful protections against cyber attacks (inadvertent and deliberate) that could affect distribution power system reliability and efficiency, by being very sensitive to anomalies in power system behavior. If such an anomaly is detected rapidly, then ameliorating actions can immediately be started to delay or isolate the attack, survive during the attack, and retain timestamped audit logs of all anomalous activities.

4.2 Use of AMI Systems as Source of Critical Security-Related Information

AMI systems reach out to customer sites and possibly other areas where utility power system equipment is located. They thus form some of the most powerful means for detecting and alarming power system anomalous behavior that could indicate a cyber attack, whether deliberate or inadvertent. This capability is (not yet) part of most AMI system designs except as vague notions that this type of power system data could be made available.

One possible design for using AMI systems for power system information is to select a small set of critically located meters which should have their voltage level, var measurements, and other key power system information. This small set would be used to detect critical anomalies that might indicate a cyber security attack.

4.3 Compensating Security Measures

Utilities worry how to provide security for legacy equipment and systems, particularly those that are compute-constrained and/or communication media-constrained. It is financially and logistically impractical to replace older power system equipment (even that equipment deemed a Critical Asset) just to add security measures. Compensating security solutions using existing power system management technologies can assist in addressing these legacy system constraints by using power flow-based analysis to detect (inadvertent or deliberate) security anomalies and by using traditional protective relaying and switching to isolate areas with security problems.

In addition, power systems must continue to operate as reliably as possible, so procedures and technologies are needed to manage the power system during a security attack – again something that SCADA, EMS, and DMS systems are designed to perform. Layered security is critical not only to prevent security attacks, but also to detect actual security breaches, to cope and survive during a security attack, to mitigate any the damage caused by them, and to log all events associated with the attack.

Most traditional “IT” security measures, although important where they can be deployed, cannot address all of these power system issues. They are typically focused on preventing attacks, and usually have minimal capabilities to survive during an attack, since the primary action is to turn off the attacked systems – an action that is impossible for operational systems in the power industry.

One method for addressing these problems is to use existing and expanded power system management technologies as a valid and very powerful method of security management, particularly for detecting, coping with, and logging security events.

4.4 Examples of Using Power System Management for Security Management

Examples include:

- **Utilize normal SCADA capabilities**, such as alarm handling, integrity scans, communications monitoring, data entry validation, etc., to detect and log equipment failures, communication failures, invalid data, and other (typically inadvertent) security compromises.
- **Utilize and expand existing SCADA systems** to monitor additional security-related points, such as opening doors and gates, status of IEC equipment (such as loss of power, processor restarts, application crashes, etc.), status of networks (unexpected requests, traffic anomalies, availability performance) in additional to the normal communications notifications of permanent failures.

- **Extend typical Area of Responsibility (AoR) SCADA capabilities to Role-Based Access Control**, to tighten permissions, log all invalid access events, and identify not only roles but individuals.
- **Expand transmission and sub-transmission power-flow analysis** to identify anomalous power system behavior such as unexpected shifts of load and generation patterns, unexpected state estimation mismatches between monitored data and estimated data, and abnormal power flow contingency analysis results to identify unexpected situations.
- **Design and/or expand the Distribution Management System** to include judiciously selected power system information from the AMI system, such as local loads, DER generation, voltage levels, etc. The DMS should also receive any demand response signals and load control signals and/or "expected customer-side response schedules" resulting from these signals. Using all of this information DMS power flow applications such as distribution contingency analysis can then assess both normal and abnormal situations (due to inadvertent as well as deliberate security events).
- **Expand distribution management of customer-based DER generation and storage** to ensure not only protection against security threats, but also just to maintain current power system reliability, given the rapidly expanding implementation of DER equipment at customer sites and the fact that the distribution system has not been designed to handle either the variability of renewables as well as possible back-flow of generation.
- **Expand normal revenue protection assessment** of individual metering information to include possible tampering of multiple meters, such as failed logins to multiple meters, similar events across multiple meters (e.g. multiple unsolicited remote disconnects), unexpected restarts of multiple meters, and other patterns not normally expected.
- **Expand and tighten the normal Role-Based Access Control (RBAC)** capabilities (used in SCADA systems to split operational responsibilities and capabilities) to cover more users (human and software application), and to include the security principle of "least privilege", which provides a user with only the minimum privileges on each resource that they need to accomplish their authorized required activities.
- **Validate as reasonable all data entries and modifications** from a power system perspective, as well as authenticated as made by an authorized user.
- **Expand information alarm and event logs** not only of power system events but also of information infrastructure events and specific security events, with timestamps of the appropriate accuracy and resolution.
- **Notify a "security" operator** in addition to the power system operator of anomalous events resulting from power system management tools.

Therefore, normal and expanded power system management technologies and procedures should be seen as very valid components of security solutions. ***In fact, requiring the expanded use of these power management technologies to address security requirements may become one of the most powerful solutions to security management.***