SECURITY PROFILE FOR ADVANCED METERING INFRASTRUCTURE

Prepared for:

The AMI-SEC Task Force (UCAIug)

&

The NIST Cyber Security Coordination Task Group

Prepared by:

The Advanced Security Acceleration Project (ASAP-SG)

Managed by:

EnerNex Corporation
620 Mabry Hood Road
Knoxville, TN 37923
USA
(865) 218-4600
www.enernex.com

Version 2.1

Revision History

Rev	Date	Summary	Marked
0.46	20090918	First public draft	N
0.47	20091019	Numerous changes: • Added Revision History • Added Executive Summary • Added Table of Figures • Added Table 2 - Summary of Communications with Out-of-Scope Components • Revised Recommended Controls and added Rationale • Added example survivability control (2.17) • Minor miscellaneous edits and clarifications	N
0.48 0.49	20091021 20091030	Added Appendices A and B Misc Changes: • Moved comments to separate document • Changed UtiliSec references to SG Security • Removed several organizational controls	N N
0.50	20091118	Initial changes based on public comments and Usability Analysis team comment dispositions.	Y
0.9	20091202	Numerous changes in response to comments received from SG Security and NIST reviewers.	Y
1.0	20091210	Approved by AMI-SEC Task Force • All changes accepted • All comments removed • Updated Acknowledgements and Authors	N
1.9	20090524	Numerous changes in response to comments received.	Y
2.0	20090622	Approved by AMI-SEC Task Force • All changes accepted • All comments removed	N
2.01	20121012	Revised Table 2 line #4	Y
2.1	20121023	Accepted change to Table 2, line #4 Removed comment	N

Executive Summary

The Advanced Metering Infrastructure Security (AMI-SEC) Task Force was established August 2007 under the Utility Communications Architecture International Users Group (UCAIug) to develop consistent security guidelines for AMI. This document represents the security concerns of the AMI-SEC Task Force and provides guidance and security controls to organizations developing or implementing AMI solutions. The intent of the document is to provide prescriptive, actionable guidance for how to build-in and implement security for AMI smart grid functionality. This guidance is neutral to vendor specific implementations and architectures.

The scope of this work extends from the meter data management system (MDMS) up to and including the home area network (HAN) interface of the smart meter. Informative security guidance may be provided for systems and components relevant but beyond the explicitly designated scope. In developing this guidance, the task force examined community-established AMI use cases, evaluated risk for AMI, and utilized a security service domain analysis. The task force then modified and enhanced controls from the Department of Homeland Security to produce the recommended cyber security controls for AMI. The actionable portion of this document is the resulting catalog of controls applicable to AMI systems and components.

Table of Contents

Table of Figures

1 Acknowledgements

SG Security Working Group (WG) and AMI-SEC Task Force (TF) would like to acknowledge the work of the primary authors, contributing authors, editors, reviewers, and supporting organizations. Specifically, we would like to thank:

- ASAP-SG (Advanced Security Acceleration Project – Smart Grid)
    - Supporting utilities, including American Electric Power, BC Hydro, Con Edison Consumers Energy, Florida Power & Light, Oncor, and Southern California Edison.
    - Supporting organizations including The United States Department of Energy and the Electric Power Research Institute.
- The utilities, vendors, consultants, national laboratories, higher education institutions, governmental entities, and other organizations that have actively contributed to and participated in the activities of the SG Security WG and AMI-SEC Task Force

The SG Security WG and AMI-SEC TF would also like to thank the Department of Homeland Security (DHS) Cyber Security Division, National Institute of Standards and Technology (NIST) Computer Security Division, North American Reliability Corporation (NERC) and The Common Criteria for the works that they have produced that served as reference material for the AMI Systems Security Requirements document.

2 Authors

Len Bass

Bobby Brown

Kevin Brown

Matthew Carpenter

James Ivers

Teja Kuruganti

Howard Lipson

Jim Nutaro

Justin Searle

Vishant Shah

Brian Smith

James Stevens

Edited by: Darren Highfill

3 Introduction

The Advanced Metering Infrastructure Security (AMI-SEC) Task Force was established August 2007 under the Utility Communications Architecture International Users Group (UCAIug) to develop consistent security guidelines for the initial AMI portion of the Smart Grid. The Task Force set forth an aggressive schedule for 2008, with voluntary resources and found this was not sufficient to maintain the desired pace; therefore, several utilities expressed the need for further and faster assistance with AMI security. In response, the AMI-SEC leadership defined a project to accelerate and augment the work of the Task Force, referred to as ASAP.

The Advanced Security Acceleration Project Smart Grid (ASAP-SG) has evolved to a collaborative effort between EnerNex Corporation, multiple major North American utilities, the National Institute of Standards and Technology, and the United States Department of Energy (DOE), including resources from Oak Ridge National Laboratory and the Software Engineering Institute of Carnegie Mellon University. The Electric Power Research Institute (EPRI) played a major role in bringing their utility membership to the original ASAP project and they may do so again with ASAP-SG.

Now with the objectives defined in the American Reinvestment and Recovery Act of 2009, utilities are under greater pressure to aggressively deploy smart grid technologies and applications. Additionally the President of the United States, U.S. Congress, the Federal Energy Regulatory Commission, the DOE, and numerous other authoritative entities have identified cyber security for the smart grid as a top priority. This project addresses both the recommendation by the utilities of the Open Smart Grid Committee and government entities to take the next step to produce actionable, understandable, and targeted guidance for securing the smart grid.

3.1 Purpose

The purpose of this document is to present security concerns relevant to AMI and provide guidance and security controls to organizations developing or implementing AMI solutions for the Smart Grid. Specifically, this document aims to facilitate the procurement process by serving as reference material for utilities in the Request-for-Proposal process as well as vendors looking to build solutions to utility requirements. The intent of the document is to provide prescriptive, actionable guidance for how to build-in and implement security for AMI smart grid functionality. This document provides a tailored security profile based on AMI use cases. For ease of management, functions and components are first aggregated into security domains. The specification is neutral to vendor specific implementations and architectures.

3.2 Scope

The intent of this document is provide normative security guidance for AMI systems from the meter data management system (MDMS) up to and including the HAN interface of the smart meter. The controls selected and adapted to AMI in this document are limited to the components and interfaces that have the primary purpose of supporting AMI. Architecturally the scope represents the components and communications from the MDMS and its related components to the smart meter. This document does not cover organizational security controls that are superfluous to the organization.

Informative security guidance may be provided for AMI related components that extend beyond the external interfaces of the MDMS and smart meter.

3.3 Approach

The ASAP-SG team took the following steps to develop recommended cyber security controls for AMI. This document also explains the process for examining risk and cyber security concerns within the electric power industry.

1. Examination of AMI Use Cases
2. Evaluation of risk for AMI
3. AMI security service domain analysis
4. Modification and enhancement of DHS controls

Many AMI systems share commonality at the logical level, although systems will vary among utilities based on technology choices and features they intend to support. Publicly available material was used and reviewed as a reference to the logical structure of AMI systems. The primary source used for UML use cases, scenarios and sequence diagrams was www.smartgridipedia.org. From this analysis, the ASAP-SG team extracted a logical architecture and examined the communications among logical and physical components.

The ASAP-SG team evaluated the risks associated with AMI components and interfaces. Where necessary, components were decomposed into sub-components where application of security controls differ and are further elaborated later in this document. Cyber security concerns

surrounding current AMI components and technology were taken in consideration such as key management, firmware assurance and protection, and trust between intra- and inter-organizational users and objects.

Security controls were selected based on applicability to components and messages of AMI scenarios that were studied. Security service domains were used as a tool to further characterize these components with respect to additional security considerations. The assigning of components to AMI security service domains, examination of processes, communication and security considerations were used in the selection of requirements for each component.

3.4 Audience

The primary audience of this document is for organizations that are developing or implementing AMI solutions. This document is written at the normal level of utility security experience for system owners, system implementers and security engineers. The user is assumed to be experienced at information asset risk estimation. The user is further assumed to be knowledgeable in developing security requirements and guidance.

3.5 Disclaimer/Status

Please note that the recommended controls listed in this document are adaptations of the DHS controls as appropriate for AMI security. The DHS control section numbers are only provided for traceability, and not intended to indicate that the controls in this document are the DHS controls themselves. When the ASAP-SG team created controls for which there was no DHS counterpart, the "ASAP-" prefix is used instead of "DHS-".

Note: The syntax in this document follows the following conventions

- The word shall, equivalent to “is required to”, is used to indicate mandatory requirements, strictly to be followed in order to conform to the standard and from which no deviation is permitted.
- The word recommended is used to indicate flexibility of choice with a strong preference alternative.
- The use of the word must is deprecated and shall not be used when stating mandatory requirements. The word must is only used to describe unavoidable situations.
- The word should, equivalent to “is recommended that,” is used to indicate among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; That a certain course of action is preferred but not required; That (in the negative form) a certain course of action is deprecated but not prohibited.
- The word may, equivalent to “is permitted,” is used to indicate a course of action permissible within the limits of this standard.
- The word can, equivalent to “is able to,” is used to indicate possibility and capability, whether material or physical.

4 Domain Analysis

Security requirements were selected based on the domain analysis described in this section. While AMI systems will vary among utilities, based on technology choices and features they intend to support, much is common at the logical level. A good summary of features and logical structure can be found in publicly available and reviewed material.

We began our analysis with a review of use cases and related detailed scenarios provided by the AMI Enterprise community (based on work contributed to the community by SCE). This analysis is discussed in section 4.1.

From this analysis, we extracted a logical architecture (presented in section 4.2) summarizing the communications among logical components. These logical components are further elaborated in section 4.3.

Finally, we used security domains (described in section 4.4) to further characterize these components with respect to additional security considerations. This aggregate understanding of the AMI domain, the components within the domain, and their patterns of communication and security considerations were used in the selection of requirements for each logical component.

4.1 Use case and scenario analysis

Several collections of use cases have been developed by the community, but we decided to work from the AMI Enterprise use cases documented on SmartGridiPedia[1]. This decision was driven by the following criteria

[1] http://www.smartgridipedia.org/index.php/Use_Cases_with_Integration_Requirements

- rich information content (in the form of a collection of detailed scenarios for each use case)
- good coverage of AMI features
- community review of the use cases and scenarios, reflecting some degree of community consensus in the AMI space
- public availability

Given the scope of this security profile, we restricted our attention to those use cases describing AMI features and business flows. Specifically, these are scenarios B1-B4, Consolidate Demand Response and Load Control, C1-C4, D4, I1-I3, and S1.

This set of scenarios is not, however, assumed to be complete. Other AMI features or alternate business flows are likely. From the available material, however, we were able to extract a great deal of information for how typical components of an AMI system interact, what types of information or control signals flow between components, and which components are isolated from each other.

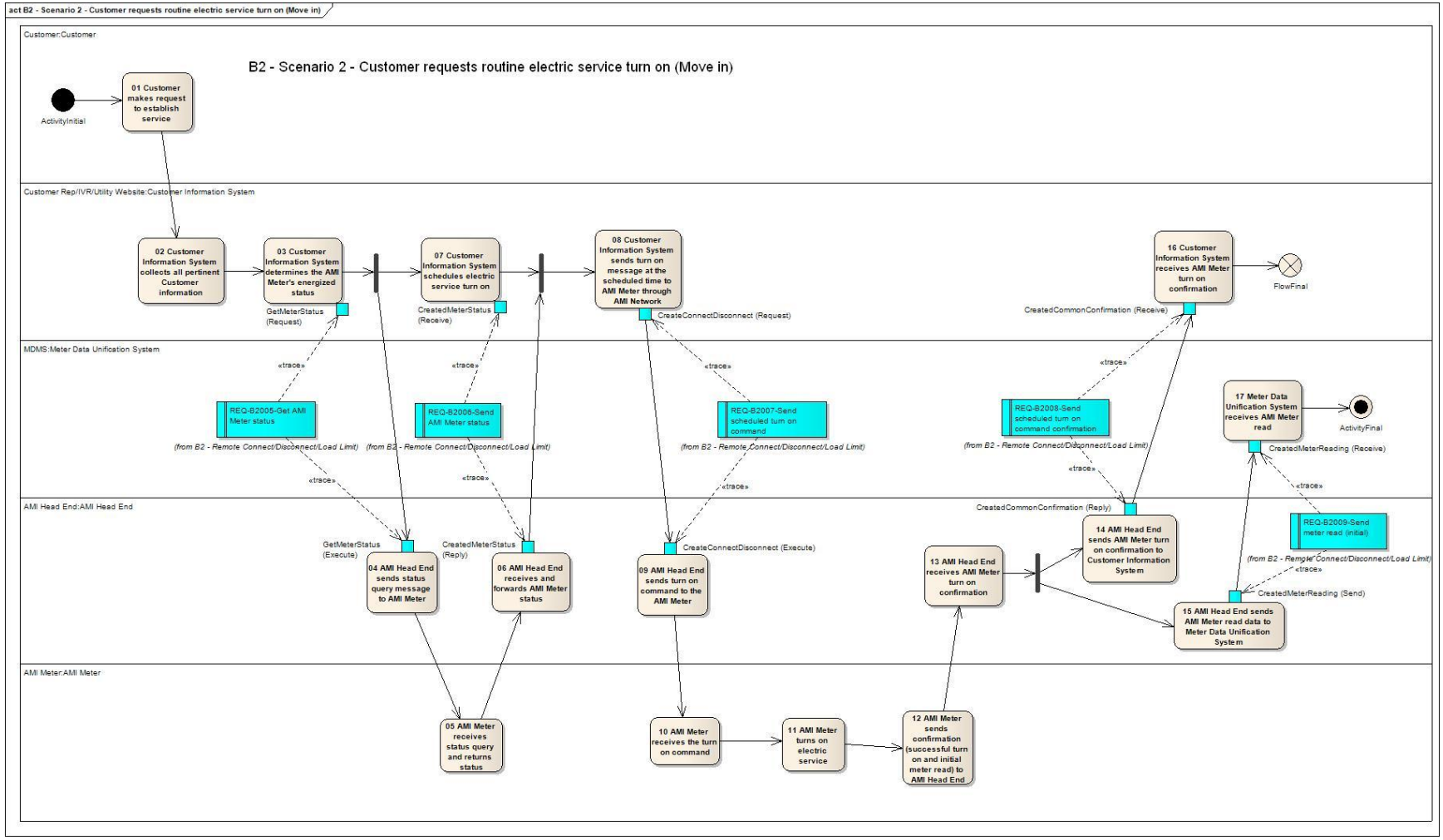

Figure 1: A UML activity diagram for Scenario 2 of use case B2

Figure 1 shows one of the scenarios as an example. From diagrams of this kind, we extracted

- Components: each swim lane depicts a different entity involved in the business flow captured in the scenario's activity diagram. Some components represent system components, while others represent human actors. For our purposes, we restricted our attention to system components. Additionally, some components were deemed outside the scope of the AMI profile.
- Communication: arrows between nodes often represent some communication of information or control signals between components. Other times, arrows simply represent the sequence of activities. Some interpretation was necessary. The key information extracted at this point was the nature of information and control exchanged between components.

Some inconsistencies and oversights were encountered in analyzing the use cases and scenarios. For example, in scenario 9 of use case B1, a meter is shown communicating with the MDMS without going through a Head End. This was inconsistent with many other scenarios, and assumed to be an oversight. Such corrections were made in several places to arrive at a consistent logical architecture.

4.2 Logical architecture

A logical architectural view depicts logical components and their interactions. By logical components, we refer to conceptual elements defined by common functionality. A logical architectural view does not attempt to capture deployment information, such as allocation of functionality to hosts or network segments. Nor does it attempt to capture all terminology and physical configurations represented by different products.

The logical architectural components have only the meaning defined in this document, regardless of how some other party may define the same terms.

As such, any product implementing the function of a logical component, shall satisfy all security requirements identified in Section 5 that apply to that component—regardless of whether the product uses that component's name or whether it implements the functions of multiple components. Products that implement the functions of multiple components shall satisfy all security requirements of each component whose functions it implements.

This view was extracted from the use cases and scenarios described in Section 4.1, with some simplifications. In these figures, we spotlight the communications between components that are in-scope for the AMI profile and between in-scope components and out-of-scope components. We omit all communications between out-of-scope components. For example, while the source material describes the nature of some communications between an Enterprise Asset Management component and a Workforce Management System, this information omitted to allow focus on the components that are in the scope of this profile. Likewise, we did include information on interactions between human actors[2].

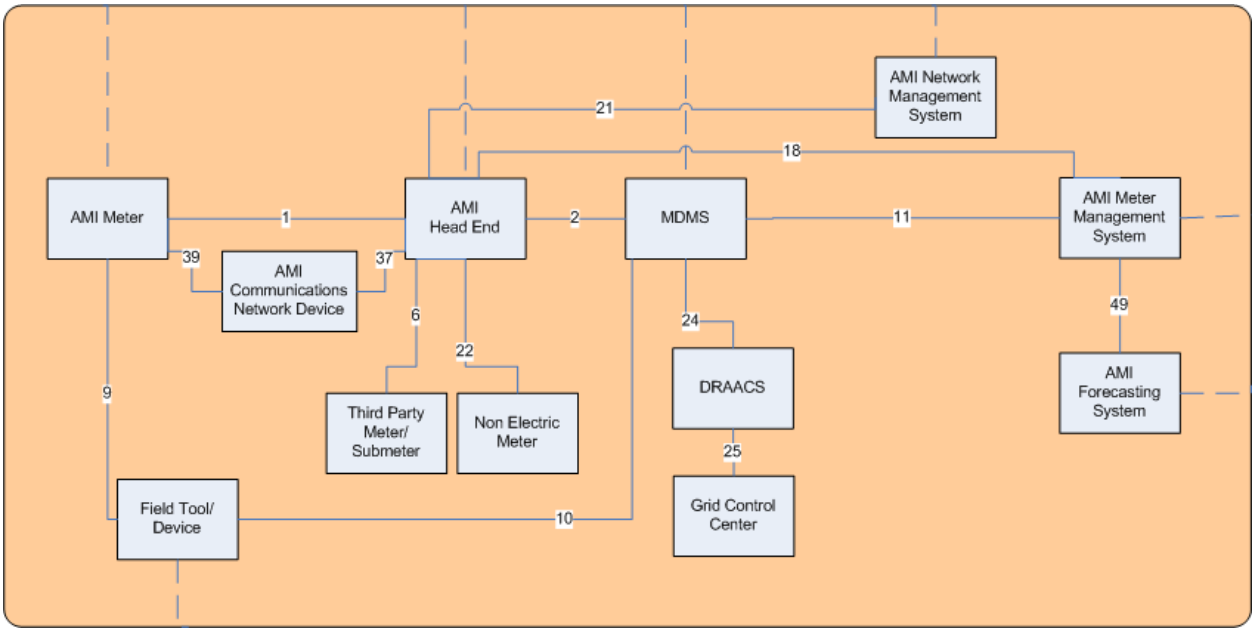

Figure 2: AMI Logical Architectural View (Internal Perspective)

Figure 2 shows a draft of the resulting logical architecture. This presentation of the view focuses on interactions between components that are in-scope for this profile. Each point of interaction between components is represented by a numbered line. Dashed lines represent interactions between in-scope components and out-of-scope components or actors. Table 1 summarizes the communications between in-scope components; each summary presents a variety of communications and commands communicated between the components without attempting to be complete[3].

[2] After this filter step, several actors were left "orphaned" in the diagram—interacting with no other actor or in-scope component. They—Customer, Customer Representative, DG Evaluation Team, and Third Party Organizations—were removed.

[3] A listing of the raw material used to compile these summaries is found in Appendix B.

Line #	Direction	Summary of communication
1	to AMI Meter	Meter read requests, turn on/off commands, pricing data, provisioning requests, firmware updates, prepayment information
	to AMI Head End	Meter read data, various meter events (e.g., tampering, outage, and restoration), various confirmations (e.g., meter turn on/off, load shed start/end, and meter provisioning), HAN communication, error logs
2	to MDMS	Meter read data, various meter events and confirmations, HAN equipment responses, outage and restoration notifications, event logs
	to AMI Head End	Meter read requests, load shed commands, planned outage information, HAN equipment commands
6	to AMI Head End	Meter read data
	to Third Party Meter/Submeter	Meter read requests
9	to Field Tool/Device	Stored meter data (including meter read data and ID) and logs, turn on/off confirmation, AMI system registration success, meter test results
	to AMI Meter	Request for all meter data and logs, credentials for field person using Field Tool/Device, turn on/off commands, meter configuration data, request communication test and self-test results
10	to MDMS	Stored meter data
	to Field Tool/Device	None identified
11	to AMI Meter Management System	Problem meters report, meter service order request, meter read data
	to MDMS	Meter read requests, closed meter order status
18	to AMI Meter Management System	Various meter events (e.g., intrusion, inversion, and customer load detected), meter status, meter location change or network disconnection, meter service order request, confirmation of firmware update download
	to AMI Head End	Non-electric meter read requests, meter reconfiguration, updated firmware, command to execute firmware update, HAN device ping requests
21	to AMI Network Management System	Meter events, activity records
	to AMI Head End	Non-electric meter read requests[4]
22	to AMI Head End	Meter read data, establish connection confirmation, non-electric meter events
	to Non Electric Meter	Meter read requests, establish connection commands, meter event monitoring requests
24	to MDMS	Load shed control notification
	to DRAACS	Load shed event end
25	to DRAACS	Load control request
	to Grid Control Center	Load shed report

[4] This probably shouldn't go from both AMI Management System and AMI Network Management System to Head End.

Line #	Direction	Summary of communication
37	to AMI Head End	Power outage and restoration notifications, meter last gasp messages, collector running on battery messages, collector power restored messages
	to AMI Communications Network Device	None identified
39	to AMI Communications Network Device	Meter last gasp messages
	to AMI Meter	None identified
49	to AMI Meter Management System	Meter inventory requests
	to AMI Forecasting System	Meter inventory responses

Table 1: Summary of Communication in AMI Logical Architectural View (Internal Perspective)

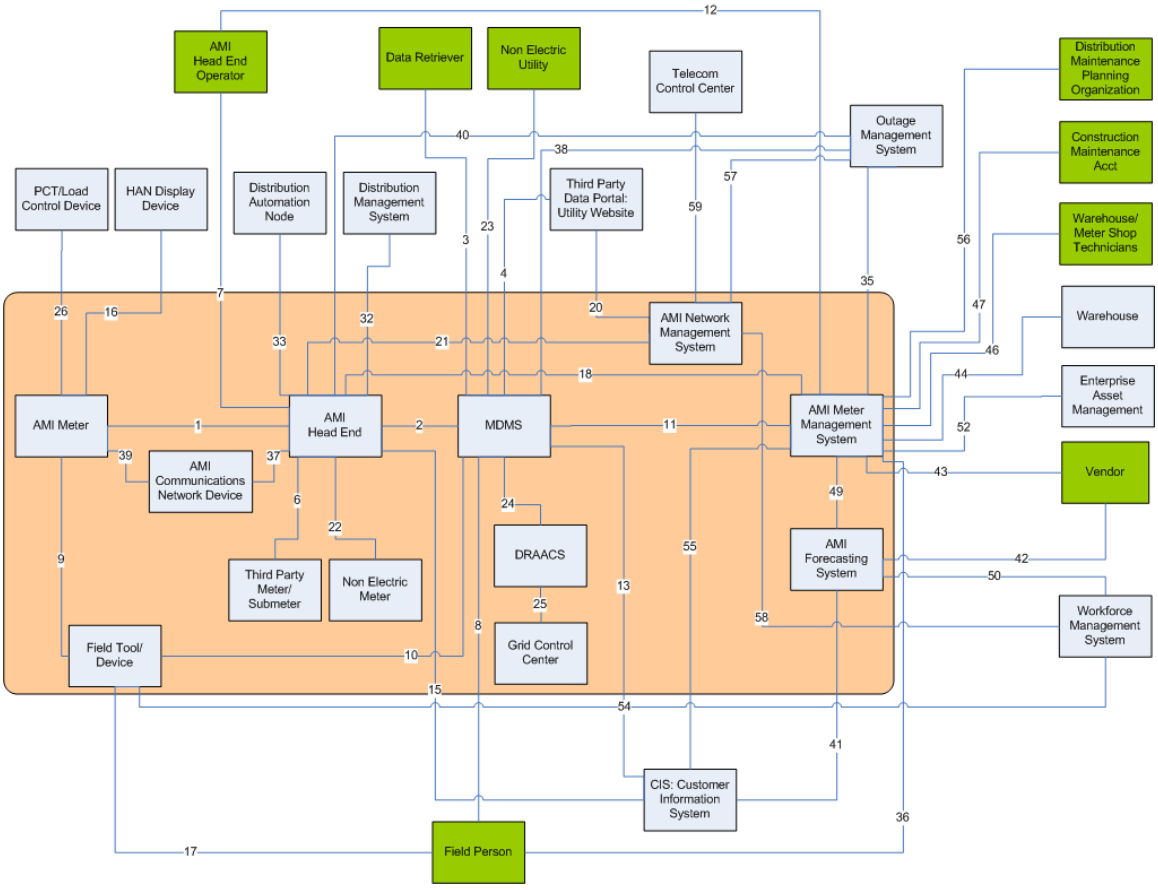

Figure 3: AMI Logical Architectural View (Full Perspective)

Figure 3 shows an expansion of this view in which out-of-scope components and actors are included (each dashed line is replaced by one or more numbered line). Interactions between out-of-scope components and actors are not shown. Table 2 below summarizes

the communications between in-scope components and out-of-scope components and actors; each summary presents a variety of communications and commands communicated without attempting to be complete[5].

Line #	Direction	Summary of communication
3	to MDMS	Meter read requests, meter event acknowledgements, data requests
	to Data Retriever	Meter read data, meter events, requested data, service order results
4	to MDMS	Meter read data requests, non-electric meter event monitoring requests, customer energy data requests, customer HAN equipment responses
	to Third Party Data Portal	Meter read data, non-electric meter events, customer energy data, customer HAN equipment responses
7	to AMI Head End	None identified
	to AMI Head End Operator	Meter reading report (regarding non-responsive meters)
8	to MDMS	None identified
	to Field Person	Pickup read requests
12	to AMI Meter Management System	Schedule upgrades
	to AMI Head End Operator	Meter service orders
13	to MDMS	Billing determinant requests, prepayment requests, DG enrollment information
	to CIS	Billing determinants, prepay meter events (i.e., credit mode), successful meter program confirmations, unexpected/unauthorized DG notifications
15	to AMI Head End	Various commands (on demand turn off, scheduled turn on/off, load limit), meter energized status requests, electric price data, meter provisioning requests, various messages (informational, prepayment service, rate change)
	to CIS	Various confirmations (successful turn on/off, load limit, meter provisioning request, HAN communication), energized meter status
16	to AMI Meter	Various confirmations (event notifications, event start/end, HAN communication), prepayment status receipt
	to HAN Display Device	Various notifications (scheduled turn off, load limit, load control event), electric price data, energy consumption data, various messages (informational, test, planned and unplanned outage), prepayment status, prepay meter event (i.e., credit mode)
17	to Field Tool/Device	Meter ID confirmation, close out work order, report marginal coverage (soft registration), toggle electric service
	to Field Person	Confirmation of turn on/off electric service, meter ID match, meter read data, success of AMI system registration, work order alert
20	to AMI Network Management System	Non-electric meter read requests

[5] A listing of the raw material used to compile these summaries is found in Appendix A.

Line #	Direction	Summary of communication
	to Third Party Data Portal	None identified
23	to MDMS	None identified
	to Non-electric Utility	Identification of non-electric meters where no data is received
26	to AMI Meter	Various confirmations (event start/end, notification), customer HAN equipment response
	to PCT/Load Control Device	Load control event notification, event start/end message, customer HAN equipment commands
32	to AMI Head End	Power quality data requests, real-time data requests (volts, watts, PF, etc.), change of state commands (cap bank on/off)
	to Distribution Management System	Power quality events, power quality data responses, real-time data responses (volts, watts, PF, etc.)
33	to AMI Head End	None identified
	to Distribution Management System	Change of state commands (cap bank on/off)
35	to AMI Meter Management System	Meter service orders
	to Outage Management System	None identified
36	to AMI Meter Management System	None identified
	to Field Person	Meter service orders
38	to MDMS	Planned outage information
	to Outage Management System	Power outage and restoration notifications
40	to AMI Head End	None identified
	to Outage Management System	Meter last gasp messages, collector running on battery messages, collector power restored messages
41	to AMI Forecasting System	Quantity and types of meters to order, meter change information
	to CIS	Customer notification of meter change information
42	to AMI Forecasting System	None identified
	to Vendor	Quantity and types of meters to order
43	to AMI Meter Management System	Add meter asset requests
	to Vendor	None identified
44	to AMI Meter Management System	None identified
	to Warehouse	Expected meter arrival
46	to AMI Meter Management System	Meter receipt confirmations, meter test results, meters ready for deployment
	to Warehouse/Meter Shop Technicians	None identified
47	to AMI Meter Management System	None identified
	to Construction Maintenance Account	Dispatch of meter and communications equipment
50	to AMI Forecasting System	None identified

Line #	Direction	Summary of communication
	to Workforce Management System	Meter service orders
52	to AMI Meter Management System	Close out meter service orders
	to Enterprise Asset Management	Meter service orders
54	to Field Tool	Meter service orders
	to Workforce Management System	Work order results
55	to AMI Meter Management System	Meter service order requests, HAN device asset IDs
	to CIS	None identified
56	to AMI Meter Management System	Meter testing service order requests
	to Distribution Maintenance Planning Organization	None identified
57	to AMI Network Management System	None identified
	to Outage Management System	Outage record requests, activity records
58	to AMI Network Management System	None identified
	to Workforce Management System	Work order requests
59	to AMI Network Management System	None identified
	to Telecom Control Center	Outage record requests

Table 2: Summary of Communications with Out-of-Scope Components

There are several remaining issues to be resolved in ongoing validation activities, such as

- Can any meter communication go directly to the AMI Head End, or must all communication be routed via the AMI Communications Network Device? Note that these questions apply to all three varieties of meters in the diagram.
- What is the distinction between the AMI Meter Management System and the AMI Network Management System? Have these been consistently separated?

4.3 Component definitions

The following sections provide functional definitions of the logical components used in this document. Throughout this document, there are many passages that are applicable to all of the components defined in this section. In such cases, "AMI component" or "components of AMI systems" is used to represent any of these logical components.

4.3.1 AMI Communications Network Device

The AMI Communications Network device relays, routes, aggregates, or otherwise enables and facilitates communication between AMI components in the field and the utility operations center. This component carries all information exchanged by the operations center and field devices.

4.3.2 AMI Forecasting System

The AMI Forecasting System tracks the number of meters available for deployment and maps the inventory to anticipated deployment schedule. It maintains an appropriate level of meter inventory.

4.3.3 AMI Head End

The AMI Head End is responsible for two-way communications with AMI Meters to retrieve data and execute commands. It balances load on the communications network resulting from scheduled meter reads. It retries meters during communications failures and monitors the health of the advanced metering infrastructure. It also remotely manages and implements firmware updates, configuration changes, provisioning functions, control and diagnostics.

4.3.4 AMI Meter

An AMI Meter is an advanced electric revenue meter capable of two-way communications with the utility. It serves as a gateway between the utility, customer site, and customer's HAN devices and/or load controllers. It measures, records, displays, and transmits data such as energy usage, generation, text messages, and event logs to authorized systems. It may optionally include a disconnect switch that can be used to remotely provide or disconnect service.

AMI Meters are deployed on devices located in the field (e.g., on the side of a customer's home), and as such have limited physical protection.

4.3.5 AMI Meter Management System[6]

An AMI Meter Management System acts as a global data repository for information about each AMI Meter. It tracks deployment and operational status of meters. It also provides firmware updates for meters. An AMI Meter Management System is supply chain centered as opposed to the MDMS, which is focused on metrology (usage) data.

4.3.6 AMI Network Management System[7]

An AMI Network Management System acts as a global data repository for information about each AMI communication device, configurations of individual devices, and

[6] This component was labeled MDMS: AMI Management System in the source scenarios.
[7] This component was labeled MDMS: AMI Network Management System in the source scenarios.

configuration of the network as a whole. It also tracks operational status of AMI communications.

4.3.7 Demand Response Analysis and Control System (DRAACS)

A DRAACS sends demand response event notifications to meters and load control devices through the AMI system. It provides demand response options to operators, market traders, etc. based on predefined groupings of customers and statistical analysis of how those customers have responded in the past. In addition the DRAACS will need to be able to collect shed-able load from the premises.

4.3.8 Field Tool/Device

Field tools and devices are portable computing systems used by field personnel to connect to components in the field to perform maintenance, upgrades, diagnostics, and similar activities. It has a wireless connection to utility systems, which communicates information utility field personnel may need to perform installations or other service.

4.3.9 Grid Control Center

A Grid Control Center component comprises the utility's operations centers; real-time data and software applications used by those centers (e.g., EMS and SCADA); displays used to facilitate decision making; and applications outside of the operations center that interact with applications used for grid control.

4.3.10 Meter Data Management System (MDMS)[8]

An MDMS aggregates, validates, estimates and permits editing of meter data such as energy usage, generation, and meter logs. An MDMS stores this data for a limited amount of time before it goes to a data warehouse and makes this data available to authorized systems.

4.3.11 Non-Electric Meter

Non-electric Meters are components used for metering non-electric services (e.g., gas and water meters). Non-electric Meters sometimes use AMI networking infrastructure to provide information back to non-electric utilities. Like AMI Meters, Non-electric Meters are deployed in the field, and as such have limited physical protection.

4.3.12 Third Party Meter/Submeter

A Third Party Meter/Submeter is a metrology device that allows for the monitoring of usage on a portion of a distribution network past (at a finer granularity) a main meter. A submeter may not be owned by the utility. Third Party Meters/Submeters are deployed in the field, and as such have limited physical protection.

---

[8] This component was labeled MDMS: Meter Data Unification System in the source scenarios.

4.4 AMI Security Service Domains

We built much of our analysis off the work performed by the AMI-SEC Task Force in 2008, especially with regard to security domains – a concept introduced to the electric power sector by the IntelliGrid Architecture Project in 2003[9]. A security domain is an area within which one may assume a relatively consistent set of constraints and expectations with respect to security. Security domains are thereby used as a tool for analyzing devices, applications, and components for characteristics that would beg specific control requirements. However, a thorough comprehension of the security domain concept as an analysis tool is not essential to the application of the control recommendations, nor is an understanding the security domains presented herein. We used security domains as one tool among several to inform our decisions about recommended controls, and offer these comments as insight into our selection of recommendations.

4.4.1 Delineation of Domains

The 2009 AMI Security Service Domains diagram is very similar to the original drawing from the AMI System Security Requirements[10] with one formatting change and one technical change. The drawing has been rotated 90 degrees counter-clockwise to facilitate easier reading, and the Utility Enterprise domain now extends to interface directly with the Managed Network domain.

[9] THE INTEGRATED ENERGY AND COMMUNICATION SYSTEMS ARCHITECTURE, EPRI, Palo Alto, CA and Electricity Innovation Institute, Palo Alto, CA: 2003

[10] AMI System Security Requirements v1.0 Revised, UCA International Users Group – AMI-SEC Task Force, Knoxville, TN: 2008

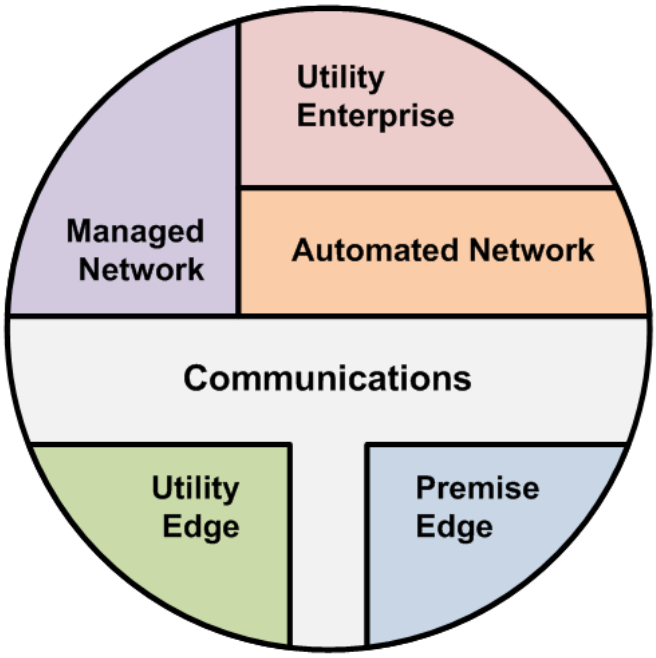

Figure 4: AMI Security Service Domains

Each of the AMI Security Service Domains represents a comprehensive set of concerns including (but not limited to) ownership, control, physical access, logical access, information sensitivity, and business functionality. Physical assets are distributed throughout the drawing and are not presumed to move or change domain. Information flows across the drawing, passing from one domain to another by crossing the boundaries between domains and is not presumed to "jump" a domain in its path.

The drawing assumes other utility enterprise applications beyond AMI such as Outage Management and Customer Information will connect through the Utility Enterprise domain. Field applications such as the Home Area Network or other utility meters (i.e., gas or water) will connect through the Premise Edge or Utility Edge domain, respectively, as discussed below.

4.4.2 Domain Characteristics

While a thorough examination of each AMI Security Service Domain provides the security analyst with a strong tool for evaluation of controls, such a discussion is not captured herein and is not essential to implementation of these recommendations. We do, however provide a brief description for each of the AMI Security Service Domains below. In essence, the questions the AMI Security Service Domains are trying to address are:

- Where does it reside in terms of utility facilities and physical environmental controls?

- Who owns it?
- Who is responsible for operating it?
- With what (types of) systems does it interface?

The AMI Security Service Domains also serve as a mechanism by which to level security requirements across multiple logical components. This is done in the interest of preventing "hop scotching" from an insignificant component (e.g., a print server) to a significant component (e.g., customer database). We endeavored to treat all components within a security domain equally to the extent practical or applicable for the component. The NERC CIP standards[11] employ a similar concept with Critical Cyber Assets and Cyber Assets within the same Electronic Security Perimeter.

We have also included some questions to help the analyst determine whether a component falls into a given domain. In examining these questions, we used the following rules:

1. A component should satisfy all the questions posed for a particular domain.
2. If a component satisfies all questions for more than one domain, the component should be decomposed further until each sub-component maps to one and only one domain.
3. If a component does not satisfy all the requirements of any domain, something is wrong and we need to either:
    a. re-examine the asset
    b. re-examine our delineation of domains
    c. determine the component is out-of-scope

Using this approach, we were able to clarify our understanding of each component and several key characteristics that influenced subsequent control selection.

[11] North American Electric Reliability Corporation. 2006, June 1. NERC Critical Infrastructure Protection (CIP). Retrieved from http://www.nerc.com/page.php?cid=2|20

Security Domain	Description	Criteria	Examples (AMI)
Utility Enterprise	Processing and/or storage of business application data, and support of utility enterprise applications	Is the asset centrally located (vs. field deployed and distributed)? (Y) Does the asset control business operation (i.e., not communications behavior) of assets or provide business processing of data from assets in the Utility Edge domain? (Y) Does the asset interface with utility enterprise applications (or their assets)? (Y)	Meter Data Management System (MDMS), Customer Information System (CIS), SCADA
Automated Network	Collection, transmission, translation, staging, and associated transformation of field communications	Is the asset centrally located (vs. field deployed and distributed)? (Y) Does the asset provide an interface for assets in the Utility Enterprise domain to access assets in the Utility Edge or Premise Edge domains? (Y) Does the asset provide a singular logical point of interface to assets in the Utility Enterprise domain for business data from assets in the Utility Edge or Premise Edge domains? (Y)	AMI Head End, AMI Network Management System, SCADA systems
Managed Network	Oversight, administration, and control of Automated Services and Communication Services	Does the asset provide an interface for monitoring or manipulation of functions performed by assets in the Automated Network or Communications domains? (Y)	Management Console
Communications	Relaying, routing, and aggregation of field communications	Is the asset field deployed? (Y) Is the asset part of the communications mechanism connecting centralized utility applications with distributed, field deployed assets? (Y)	Field Area Network (FAN), Backhaul

Security Domain	Description	Criteria	Examples (AMI)
Utility Edge	Support of field deployed utility equipment and devices (i.e., monitoring, measurement, and/or control)	Is the asset field deployed? (Y)	Metrology, Disconnect Switch
		Is the asset owned and operated by the utility? (Y)	
		Does the asset perform a function critical or essential to the operations or business of the utility? (Y)	
Premise Edge	Support of customer equipment and devices (i.e., provisioning, monitoring, measurement, and/or control)	Is the asset field deployed? (Y)	Home Area Network (HAN) Interface
		Does the asset provide an interface for the customer (or their assets)? (Y)	

Table 3: AMI Security Service Domain Characteristics

It is important to note that the AMI Security Service Domains form logical points of demarcation with regards to the system. Many commonly found devices and applications in AMI systems (and sometimes components whose functions they implement) actually span two or more domains. Where this occurred, we decomposed the component further into discrete sub-components until each sub-component could fit into one and only one domain. Recommended controls may be associated with logical components or sub-components. Further work will drive recommendations in some areas to increased levels of detail and prescription and may refine allocation of controls from components to sub-components.

One particular example of interest is the AMI Meter, which as a whole would span the Communications, Utility Edge, and Premise Edge domains. We therefore decomposed this component into the metrology and disconnect switch (if present) in the Utility Edge domain, the Field Area Network interface in the Communications domain, and the Home Area Network interface in the Premise Edge domain. Each of these sub-components and therefore any product implementing their function shall satisfy all security requirements identified in Section 4.3 that apply to that sub-component. The end result is that an AMI Meter inherits security requirements derived from the characteristics and constraints of the Communications, Utility Edge, and Premise Edge domains. Note, while this discussion focuses on the AMI application, a logical extension to other applications utilizing the AMI transport infrastructure can be drawn utilizing the same methodology.

4.4.3 Domain Analysis – Significance, Relevance, and Influence

The AMI Security Service Domain proved to be a strong tool for driving convergence of understanding regarding security constraints and expectations of the logical components identified. By examining these components in light of multiple security characteristics simultaneously (as guided by the AMI Security Service Domains), we were able to better understand their relevant attributes and motivate selection of controls.

Controls in this document were selected and/or modified to address mission-level needs identified in the referenced AMI system use cases. The resulting controls found throughout Section 5 represent the superset of all controls recommended for AMI systems and components. Not all of these controls will be relevant or even technologically practical for every AMI component.

Appendix A bridges this gap by mapping controls to applicable components. Decisions regarding applicability were based on the following criteria:

- Role of the component in the logical architecture (including its functional role in use cases and its interactions with other components and actors),
- AMI Security Service Domain for the component,
- Characteristic needs for the AMI Security Service Domain,
- Technological capability of the component, and
- Security and domain expertise relevant to components of its kind.

5 Recommended Controls

The following controls are adapted from the DHS Catalog of Control Systems Security[12] and have been modified or extended as appropriate for AMI security. The DHS control section numbers are only provided for traceability, and not intended to indicate that the controls in this document are the DHS controls themselves. When the ASAP-SG team created controls for which there was no DHS counterpart, the "AMISP-" prefix is used instead of "DHS-".

Each control in this section identifies the components of an AMI system to which it applies; this information is summarized in Appendix A. Many controls apply to all components of the logical architecture defined in Section 4; these controls refer to "AMI components" or "components of an AMI system" to indicate their applicability to all logical components defined in section 4.3.

DHS-2.8 System and Communication Protection

System and communication protection consists of steps taken to protect the AMI components and the communication links between system components from cyber intrusions. Although AMI system and communication protection might logically include both physical and cyber protection, this section addresses only cyber protection. Physical protection is addressed in Section 2.4 of the DHS controls.

[12] Department of Homeland Security, National Cyber Security Division. 2008, January. Catalog of Control Systems Security: Recommendations for Standards Developers. Retrieved from http://www.us-cert.gov/control_systems/

The organization shall ensure the AMI system and communication protection policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The AMI system and communication protection policy needs to be included as part of the general information security policy for the organization. System and communication protection procedures can be developed for the security program in general and an AMI system in particular, when required.

These documents also need to include a documented plan that covers the policies and procedures that cover a breach in security.

DHS-2.8.2 Management Port Partitioning

DHS-2.8.2.1 Requirement:

AMI components shall isolate telemetry/data acquisition services from management services.

DHS-2.8.2.2 Supplemental Guidance:

Separation may be accomplished by using different computers, different central processing units, different instances of the operating systems, different network addresses or protocol ports (e.g., TCP ports), combinations of these methods, or other methods as appropriate. Such precautions reduce the risk of allowing access to a data acquisition server and can help limit the damage of a compromised system.

Configuration and testing ports for AMI components should be disabled when not in use. Depending on the criticality of the system it may be advised that a device be physically disconnected.

Such precautions reduce the risk of allowing access to a data acquisition server and can help limit the damage of a compromised system. Configuration and testing ports for AMI components should be disabled when not in use.

Depending on the criticality of the system it may be advised that a device be physically disconnected when not in use.

DHS-2.8.2.3 Requirement Enhancements:

The AMI system management service shall be physically or logically separated from telemetry/data acquisition services and information storage and management services (e.g., database management) of the system.

DHS-2.8.2.4 Rationale:

The security requirements for access to configuration/management services on a given AMI component are greater than those required for access to telemetry/data acquisition services. Without isolation, the communication channel for access to the telemetry/data acquisition services has the potential to be leveraged to gain access to the management services. This leveraging can occur through a vulnerability in implementation, poor configuration, or other means. Ensuring separation between services limits the impact of

a vulnerability in a service with lower security requirements being leveraged to access a service with higher security requirements.

DHS-2.8.3 Security Function Isolation

DHS-2.8.3.1 Requirement:

AMI components shall use segregation of duties for security and non-security functions.

DHS-2.8.3.2 Supplemental Guidance:

AMI components shall isolate security functions from non-security functions, sometimes referred to as separation of duties, by means of partitions, domains, etc., including control of access to and integrity of the hardware, software, and firmware that perform those functions. The AMI system shall maintain a separate execution domain (e.g., address space) for each executing process. Some AMI components may not implement this capability. In situations where it is not implemented, the organization details its risk acceptance and mitigation in the AMI system security plan

DHS-2.8.3.3 Requirement Enhancements:

The AMI system shall employ the following underlying hardware separation mechanisms to facilitate security function isolation:

1. Each AMI component isolates critical security functions (i.e., functions enforcing access and information flow control) from both non-security functions and from other security functions;
2. Each AMI component minimizes the number of non – security functions included within the isolation boundary containing security functions;
3. AMI security functions are implemented as largely independent modules that avoid unnecessary interactions between modules;
4. In each AMI component, security functions are implemented as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.
5. Passwords and/or security keys should be of limited value, avoiding significant reuse of keys or passwords between different components and users. For example, compromising one key shall not allow compromise of an entire network.

DHS-2.8.3.4 Rationale:

Assurance in the integrity of the security functions implemented by an AMI component is necessary for achieving security objectives. Isolating security functions from non-security functions prevents access to the non-security functions from leveraged to compromise the security function. This leveraging can occur through a vulnerability in implementation, poor configuration, or other means. Ensuring separation between functions limits the impact of such a vulnerability.

DHS-2.8.4 Information Remnants

DHS-2.8.4.1 Requirement:

AMI components shall prevent unauthorized or unintended information transfer via shared system resources.

DHS-2.8.4.2 Supplemental Guidance:

Control of information system remnants, sometimes referred to as object reuse, or data remnants, should prevent information, including cryptographically protected representations of information previously produced by the AMI system, from being available to any current user/role/process that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system. Such information should be cleared before freeing the resource for other use.

DHS-2.8.4.3 Requirement Enhancements:

None.

DHS-2.8.4.4 Rationale:

The purpose of this control is to ensure that information that requires a given privilege level for access is not exposed to individuals or processes with a lower privilege level. Implementing this control provides assurance that information security requirements are being met. DHS-2.8.5 Denial-of-Service Protection

DHS-2.8.5/ NIST SP 800-53 SC-5 Denial-of-Service Protection

DHS-2.8.5.1 Requirement:

AMI components shall protect against or limit the effects of denial-of-service attacks.

DHS-2.8.5.2 Supplemental Guidance:

A variety of technologies exist to limit, or in some cases, eliminate the effects of denial-of-service attacks. For example, network perimeter devices can filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial-of-service attacks.

DHS-2.8.5.3 Requirement Enhancements:

1. The AMI system should restrict the ability of internal or external users to launch denial-of-service attacks against other AMI components or networks.
2. The AMI system should manage excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service attacks.

3. Wireless assets and networks are also vulnerable to radio-frequency jamming and steps should be taken and personnel trained to address tracking and resolution of such issues. This may include radio-frequency direction finding and other such technologies.

DHS-2.8.5.4 Rationale:

A denial of service attack prevents AMI resources from being available as operationally required. Any AMI component that performs more than a single function or accepts inputs is susceptible.

DHS-2.8.6 Resource Priority

DHS-2.8.6.1 Requirement:

AMI components shall limit the use of resources by priority.

DHS-2.8.6.2 Supplemental Guidance:

This control does not apply to components in the system for which only a single user/role exists.

DHS-2.8.6.3 Requirement Enhancements:

None.

DHS-2.8.6.4 Rationale:

Priority protection helps prevent a lower-priority process from delaying or interfering with the AMI system servicing any higher-priority process. This helps to prevent denial and interruption of service attacks.

DHS-2.8.7 Boundary Protection

DHS-2.8.7.1 Requirement:

The organization shall define both physical and electronic security boundary(ies) for the AMI system along with other applications sharing the same environment. The establishment of security boundaries include specifying mandatory security requirements for components that reside within a given boundary. Components that reside in a single boundary shall meet or exceed the requirements for that boundary. Components that reside in multiple boundaries shall meet or exceed all of the security requirements for all boundaries in which it resides. AMI network traffic should be on AMI network segments and be part of the asset owner's network segmentation practice.

In AMI, the very concept of boundaries is problematic. Internal systems within the organization may be more easily protected than components which reside outside significant physical boundaries and controls. Meters and poll-top and other systems

without significant controls and external monitoring cannot be amply secured and should always be considered relatively untrusted.

DHS-2.8.7.2 Supplemental Guidance:

Any connection to the Internet or other external network or computer system needs to occur through managed interfaces (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels). AMI system boundary protections at any designated alternate processing/control sites should provide the same levels of protection as that of the primary site.

At this time components and systems connected to the Internet constitute a substantial increase in risk for the core functionality of the AMI system. Connections to the Internet and other public networks are discouraged for AMI systems.

The HAN is not controlled or owned by the utility, and should be treated as a hostile network by the AMI meter.

To manage risk associated with unauthorized access, the AMI system should be segmented (or compartmentalized) into smaller boundaries (or zones) to better manage the ability to control and monitor network traffic both within the AMI system and to/from the AMI system. All AMI system components within a particular boundary will typically inherit the same security controls or privileges and boundaries should be created based on the asset owner's risk appetite. AMI network traffic should be on AMI network segments and be part of the asset owner's network segmentation practice.. At a minimum, boundaries should exist between the following AMI architectural elements:

a. a. Between HAN and NAN

b. b. Between NAN and WAN

c. c. Between WAN and Enterprise AMI System Components (AMI Head End, MDMS, AMI Management System, AMI Network Management System)

d. d. Between the AMI System as a whole and all external networks and systems.

e. e. Between AMI application and any other application sharing the AMI transport infrastructure..

DHS-2.8.7.3 Requirement Enhancements:

The following guidance also applies:

1. The organization shall limit the number of access points to the AMI system to allow for better control and monitoring of inbound and outbound network traffic;
2. The organization shall not permit untrusted access;
3. Traffic in and out of the AMI system as well as between zones shall be limited to only that necessary for proper system operation and all other traffic denied by default (i.e., deny all, permit by exception);

4. The organization physically shall locate publicly accessible AMI system components to enforce segregation of subsystem data traffic with separate, physical network interfaces. Publicly accessible AMI system components include, for example, public web servers. Generally, no AMI system information shall be publicly accessible;
5. The organization shall implement a managed interface (boundary protection devices in an effective security architecture) with any external telecommunication service, implementing security measures appropriate to the required protection of the integrity and confidentiality of the information being transmitted;
6. The organization shall prevent the unauthorized release of information outside of the AMI system boundary or any unauthorized communication through the AMI system boundary when there is an operational failure of the boundary protection mechanisms.
7. Field service tools shall not interface to the meter through the HAN.
8. Organizations wishing to leverage the AMI communications infrastructure for other Smart Grid Applications shall ensure logical application separation such that there is independence and security of the traffic streams between applications. It will be up to the organization to manage traffic prioritization within the technology to ensure expected performance.

DHS-2.8.7.4 Rationale:

In a typical control system, interfaces to external systems and networks are kept to a minimum (in many cases only a single interface/access point exists) with boundary protection mechanisms employed so that inbound and outbound network traffic can be tightly controlled and monitored. The AMI system however represents a challenge due to its architecture in that it can have potentially millions of access points created by the AMI meters and the use of wireless technologies at the neighborhood Area Network (NAN) level.

Specific challenges in implementing security for an AMI system arises from the physically insecure utility NAN as well as the fact that every AMI meter represents a potential attack vector to the AMI system.. The requirements identified in the OpenHAN SRS establish the need for two way communications between the NAN and HAN to meet the industry's long term functional goals. The addition of two way communications between the NAN and the HAN introduces additional risk for unauthorized access to the AMI system. Similarly, the utility NAN, wired or wireless, will offer attackers potential entry points into the network.

For these reasons, compartmentalization of the AMI system and Smart Grid Applications coupled with boundary protection should be employed to mitigate risk and limit the impact of unauthorized access to as small of portion of the AMI system as possible..

DHS-2.8.8 Communication Integrity

DHS-2.8.8.1 Requirement:

The AMI system design and implementation shall protect the integrity of electronically communicated information.

DHS-2.8.8.2 Supplemental Guidance:

If the organization is relying on a commercial service provider for communication services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security measures for transmission integrity. When it is infeasible or impractical to obtain the necessary assurances of effective security through appropriate contracting vehicles, the organization should either implement appropriate compensating security measures or explicitly accepts the additional risk. Contracts and other legal documents with vendors should allow for security and integrity testing of products and services used in the AMI systems.

DHS-2.8.8.3 Requirement Enhancements:

1. The organization shall employ cryptographic mechanisms to ensure recognition of changes to information during transmission unless otherwise protected by alternative physical measures. The level of protection that is required is determined by the sensitivity of the data being transmitted. (e.g., protective distribution systems).
2. The use of cryptography within an AMI system will introduce latency to AMI information processing. The latency introduced from the use of cryptographic mechanisms shall not degrade functionality (including performance) of the AMI system or impact personnel safety.
3. Failure of a cryptographic mechanism shall not create a denial of service and shall maintain security in the failure mode.
4. All security related components within an AMI system shall fail to a “safe” mode which will not result in a denial of service and will maintain component security in the “safe” failure mode.
5. Alternative systems should be in place in case of such failure. AMI systems should support the objectives of availability, integrity, and confidentiality.

DHS-2.8.8.4 Rationale:

The operation of the AMI is dependent on the integrity of electronically communicated information. The integrity requirements of electronically communicated information can be violated both intentionally and unintentionally. System components that make decisions based on compromised information can lead to system instability, malfunction,

and a host of other impacts. When unacceptable impacts can be caused by a violation of integrity requirements, there is a need to implement integrity controls.

DHS-2.8.9 Communication Confidentiality

DHS-2.8.9.1 Requirement:

The AMI system design and implementation shall protect the confidentiality of electronically communicated information where necessary.

DHS-2.8.9.2 Supplemental Guidance:

The use of a third-party communication service provider instead of organization owned infrastructure may warrant the use of encryption. The use of cryptographic mechanisms within an AMI system could introduce information processing latency due to the additional time and computing resources required to encrypt, decrypt, and authenticate each message. The latency introduced from the use of cryptographic mechanisms shall not degrade functionality (including performance) of the AMI system or impact personnel safety.

DHS-2.8.9.3 Requirement Enhancements:

None.

DHS-2.8.9.4 Rationale:

Electronically communicated information in an AMI system may have confidentiality requirements because it ensures the privacy of customer and business information and it is possible that the confidentiality of electronically communicated information is required for operational integrity. The confidentiality requirements of electronically communicated information can be violated both intentionally and unintentionally and can lead to system instability, malfunction, privacy violation, loss of business advantage, and a host of other impacts. When unacceptable impacts can be caused by a violation of confidentiality requirements, there is a need to implement confidentiality controls.

DHS-2.8.10 Trusted Path

DHS-2.8.10.1 Requirement:

The AMI system shall establish trusted communications paths between the user (or agent) and the components making up the AMI system.

DHS-2.8.10.2 Supplemental Guidance:

A trusted path is employed for high-confidence connections between the security functions of the AMI system and the meter (e.g., for login or command authorization).

It is recommended that login to all component interfaces (back end systems, field devices, field service tools, etc.) should be protected by trusted path or a compensating

control. A trusted path is a mechanism by which an AMI system component can communicate directly with the Trusted Computing Base (TCB) that provides the security functions of the system. This mechanism can only be activated by the authorized user or the TCB. The TCB is the totality of protection mechanisms within an AMI system – including hardware, firmware, and software – the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of a trusted computing base to correctly enforce a security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel and parameters (e.g., a user's authorization) related to the security policy.

DHS-2.8.10.3 Requirement Enhancements:

None.

DHS-2.8.11 Cryptographic Key Establishment and Management

DHS-2.8.11.1 Requirement:

Organizations need to select cryptographic protection and key management infrastructure that matches the value of the information being protected and the AMI system operating constraints

DHS-2.8.11.2 Supplemental Guidance:

A formal written policy needs to be developed to document the practices and procedures relating to cryptographic key establishment and management. These policies and procedures need to address, under key establishment, such items as the key generation process is in accordance with a specified algorithm and key sizes are based on an assigned standard. Key generation needs to be performed using an effective random number generator (e.g., a NIST approved PRN/RNG that passes its test vectors, such as for auxiliary quantities used in generating digital signatures, or for generating challenges in authentication protocols).. The policies for key management need to address such items as periodic key changes, key destruction, and key distribution.

DHS-2.8.11.3 Requirement Enhancements:

The key management infrastructure shall be able to distinguish individual sending and receiving devices

DHS-2.8.11.4 Rationale:

If compromising the components of a cryptographic system is easier than compromising the cryptography itself, the cryptographic system will only provide protection equivalent to the protection afforded to the components of that system.

DHS-2.8.12 Use of Validated Cryptography

DHS-2.8.12.1 Requirement:

The organization shall develop and implement a policy governing the use of cryptographic mechanisms for the protection of AMI system information. The organization ensures all cryptographic mechanisms comply with applicable laws, regulatory requirements, directives, policies, standards, and guidance.

DHS-2.8.12.2 Supplemental Guidance:

Any cryptographic modules deployed within an AMI system, at a minimum, should be able to meet the Federal Information Processing Standard (FIPS) 140-2 requirements where technically and economically feasible. Assessment of the modules should include validation of the cryptographic modules operating in approved modes of operation. The most effective safeguard is to use a cryptographic module validated by the Cryptographic Module Validation Program. Additional information on the use of validated cryptography can be found at http://csrc.nist.gov/cryptval.

DHS-2.8.12.3 Requirement Enhancements:

1. The organization protects cryptographic hardware from physical tampering and uncontrolled electronic connections.
2. The organization shall select cryptographic hardware with remote key management capabilities.

DHS-2.8.12.4 Rationale:

Validating the implementation of a cryptographic algorithm requires resources that are beyond the capabilities of most utilities and vendors. Following the NIST guidance provides assurance that the selected cryptography will provide the required level of protection.

DHS-2.8.13 Collaborative Computing

DHS-2.8.13.1 Requirement:

The use of collaborative computing mechanisms on AMI components can introduce additional threat vectors that shall be mitigated. Explicit indication of use to the local users shall be provided.

DHS-2.8.13.2 Supplemental Guidance:

Collaborative computing mechanisms include, for example, video and audio conferencing capabilities or instant messaging technologies. Explicit indication of use includes, for example, signals to local users when cameras and/or microphones are activated.

AMI network traffic should be on AMI network segments and be part of the asset owner's network segmentation practice.

DHS-2.8.13.3 Requirement Enhancements:

If collaborative computing mechanisms are utilized on the AMI system, they are disconnected and powered down when not in use.

DHS-2.8.13.4 Rationale:

Collaborative computing introduces additional threat vectors to the AMI system, increasing overall risk.

DHS-2.8.14 Transmission of Security Parameters

DHS-2.8.14.1 Requirement:

The AMI components shall reliably associate security parameters (e.g., security labels and markings) with information exchanged between the enterprise information systems and the AMI system.

DHS-2.8.14.2 Supplemental Guidance:

Security parameters may be associated with the information contained within the AMI system.

DHS-2.8.14.3 Requirement Enhancements:

None.

DHS-2.8.14.4 Rationale:

Security parameters provide guidance as to the security requirements of information exchanged within the AMI system. Ensuring that security parameters are reliably associated with information being exchanged, enables the system to appropriately select and apply controls.

DHS-2.8.15 Public Key Infrastructure Certificates

DHS-2.8.15.1 Requirement:

If used, the organization shall utilize public key certificates under an asset owner defined certificate policy. Public key certificates may be issued internally under an asset owner defined certificate policy or, alternatively the organization may obtain public key certificates, under an asset owner defined certificate policy, from an approved service provider.

DHS-2.8.15.2 Supplemental Guidance:

Registration to receive a public key certificate needs to include authorization by a supervisor or a responsible official and needs to be accomplished using a secure process that verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party.

DHS-2.8.15.3 Requirement Enhancements:

Any latency induced from the use of public key certificates shall not degrade the operational performance of the AMI system.

DHS-2.8.15.4 Rationale:

The use of public key certificates can provide additional levels of assurance in the authenticity of a certificate, but care shall be taken in implementation and use. If the system supporting the key infrastructure is compromised, then the security of the system that relies on it may be put at risk.".

DHS-2.8.16 Mobile Code

DHS-2.8.16.1 Requirement:

The organization shall:

1. Establish usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the AMI system if used maliciously. The term 'potential' is defined by the asset owner and applied to internal processes;
2. Document, monitor, and manage the use of mobile code within the AMI system.

Appropriate organizational officials should authorize the use of mobile code.

DHS-2.8.16.2 Supplemental Guidance:

Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance need to apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations. Procedures need to prevent the development, modification, acquisition, or introduction of untrusted mobile code within the AMI system.

DHS-2.8.16.3 Requirement Enhancements:

All mobile code used in an AMI system must be digitally signed to validate its origin and integrity.

DHS-2.8.16.4 Rationale:

By definition mobile code is code that is originates in one location and is transported (e.g. downloaded) and executed in another. Unless the code is verified through some mechanism (e.g. digital signatures), execution of unverified code can lead to a compromise of or malfunction within the system.

DHS-2.8.17 Voice-Over Internet Protocol

DHS-2.8.17.1 Requirement:

The organization shall: (i) establish usage restrictions and implementation guidance for Voice over Internet Protocol (VOIP) technologies based on the potential to cause damage to the information system if used maliciously; and (ii) authorize, monitor, and limit the use of VOIP within the AMI system.

DHS-2.8.17.2 Supplemental Guidance:

Unless otherwise protected, VOIP technologies share the same level of protection as provided by the boundary(ies) within which the technology resides. (See DHS-2.8.8 - Boundary Protection).

AMI network traffic should be on AMI network segments and be part of the asset owner's network segmentation practice.

DHS-2.8.17.3 Requirement Enhancements:

None.

DHS-2.8.17.4 Rationale:

Including VOIP services would introduce additional threat vectors to the AMI system, increasing overall risk.

DHS-2.8.18 System Connections

DHS-2.8.18.1 Requirement:

All external AMI components and communication connections shall be identified and adequately protected from tampering or damage.

DHS-2.8.18.2 Supplemental Guidance:

Untrusted access point connections to the AMI system should be secured to protect the system, especially for administrative access. The first step in securing these connections is to identify the connections along with the purpose and necessity of the connection. This information should be documented, tracked, and audited periodically. After identifying these untrusted connection points, the extent of their protection needs to be determined. Policies and procedures should be developed and implemented to protect the

connection to the business or enterprise information system. This might include disabling the connection except when specific access is requested for a specific need, automatic timeout for the connection, etc.

DHS-2.8.18.3 Requirement Enhancements:

None.

DHS-2.8.18.4 Rationale:

External system connections provide a vector of attack into the AMI system, and therefore shall be managed to the appropriate security level to ensure the security of the AMI system.

DHS-2.8.19 Security Roles

DHS-2.8.19.1 Requirement:

The AMI system design and implementation shall use segregation of duties for security and non-security functions per asset owner practices.

DHS-2.8.19.2 Supplemental Guidance:

Security roles and responsibilities for AMI system users should be specified, defined, and implemented based on the sensitivity of the information handled by the AMI system. These roles may be defined for specific tasks and in conjunction with the type of data handled.

DHS-2.8.19.3 Requirement Enhancements:

None.

DHS-2.8.19.4 Rationale:

Defining roles and responsibilities for user ensures alignment with security requirements.

DHS-2.8.20 Message Authenticity

DHS-2.8.20.1 Requirement:

The AMI system shall provide mechanisms to protect the authenticity of device-to-device communications.

DHS-2.8.20.2 Supplemental Guidance:

None

DHS-2.8.20.3 Requirement Enhancements:

Message authentication mechanisms should be implemented at the protocol level for both serial and routable protocols.

DHS-2.8.20.4 Rationale:

Message authentication provides protection from malformed traffic, from mis-configured components, and malicious entities.

DHS-2.8.21 Architecture and Provisioning for Name/Address Resolution Service

DHS-2.8.21.1 Requirement:

AMI components that collectively provide name/address resolution services for an organization shall be fault tolerant and implement address space separation.

DHS-2.8.21.2 Supplemental Guidance:

In any mission critical network as found in an AMI system due care should be taken in terms of controlling and monitoring protocols and services.

It is recommended that a white list management approach be taken. That is all allowed protocols and services be identified and explicitly authorized with all others being filtered out of the system and denied all access. Only protocols and services necessary for the system to fulfill its primary mission should be used. It is also highly recommended that an AMI network be appropriately isolated from any general-purpose enterprise networks as they can introduce risks that could impact the critical control path of the network. There are various protocols and services that should be used in the fulfillment of any Smart Grid application; they each have their own risks and security features.

It is recommended that those risks be identified and that there be an appropriate use of mitigating technologies to address them. Many protocols and services have secure and non-secure implementations; the onus should always be on using secure forms. Examples can include:

Secure DNS vs. DNS, SSH vs. Telnet, using security extensions in DNP3, and securely tunneling any needed unsecure legacy protocols using technologies such as IPSec or a link layer encryption that might be present in the network.

DHS-2.8.21.3 Requirement Enhancements:

The use of secure name/address resolution services shall not adversely impact the operational performance of the AMI system.

DHS-2.8.21.4 Rationale:

If communication within the AMI system relies on a name/address resolution service then it shall be designed and protected to provide sufficiently reliable services.

DHS-2.8.22 Secure Name / Address Resolution Service (Authoritative Source)

DHS-2.8.22.1 Requirement:

The AMI system resource (i.e., authoritative DNS server) that provides name/address resolution service shall provide additional artifacts (e.g., digital signatures and cryptographic keys) along with the authoritative DNS resource records it returns in response to resolution queries.

DHS-2.8.22.2 Supplemental Guidance:

Host-based name resolution solutions are best practice. This requirement enables remote clients to obtain origin authentication and integrity verification assurances for the name/address resolution information obtained through the service. A DNS server is an example of AMI system resource that provides name/address resolution service; digital signatures and cryptographic keys are examples of additional artifacts; and DNS resource records are examples of authoritative data. NIST Special Publication 800-81 provides guidance on secure domain name system deployment.

DHS-2.8.22.3 Requirement Enhancements:

None.

DHS-2.8.22.4 Rationale:

If communication within the AMI system relies on a name/address resolution service then it shall be designed and protected to provide sufficiently reliable services.

DHS-2.8.23 Secure Name/Address Resolution Service (Recursive or Caching Resolver)

DHS-2.8.23.1 Requirement:

The AMI system resource (i.e., resolving or caching name server) that provides name/address resolution service for local clients shall perform data origin authentication and data integrity verification on the resolution responses it receives from authoritative DNS servers when requested by client systems.

DHS-2.8.23.2 Supplemental Guidance:

. Host-based name resolution solutions are best practice. A resolving or caching DNS server is an example of an AMI system resource that provides name/address resolution service for local clients and authoritative DNS servers are examples of authoritative sources. NIST Special Publication 800-81 provides guidance on secure domain name system deployment.

DHS-2.8.23.3 Requirement Enhancements:

The AMI system resource that implements DNS services shall perform data origin authentication and data integrity verification on all resolution responses whether or not local DNS clients (i.e., stub resolvers) explicitly request this function.

DHS-2.8.23.4 Rationale:

If communication within the AMI system relies on a name/address resolution service then it shall be designed and protected to provide sufficiently reliable services.

AMISP-2.8.1 Secure Name/Address Resolution Service (Address Resolution Tampering)

AMISP-2.8.1.1 Requirement:

The organization shall monitor address resolution traffic to identify potentially malicious patterns of behavior.

AMISP-2.8.1.2 Supplemental Guidance:

Appropriate components or programming should be included within the AMI networks to identify potentially malicious address-resolution behavior (e.g. ARP spoofing/cache poisoning). Such behavior should be identified, tracked, and the appropriate incident handling team-members alerted.

AMISP-2.8.1.3 Requirement Enhancements:

ARP spoofing and similar attacks may allow an attacker to subvert natural automated network behavior in order to allow the attacker to get "in the middle" of valid communication. Such attacks, when successful, may allow traffic to be captured, analyzed, and possibly even modified in-transit.

AMISP-2.8.1.4 Rationale:

If communication within the AMI system relies on a name/address resolution service then it shall be designed and protected to provide sufficiently reliable services.

DHS-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 AMI components is important, sensitive, and needs to be managed. AMI components 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. Care is given to protect this information

and verify that the appropriate versions are retained. Inherent in this is an information classification system that allows information assets to receive the appropriate level of protection.

The following are the controls for Information and Document Management that need to be supported and implemented by the organization to protect the AMI components.

DHS-2.9.1 Information and Document Management Policy and Procedures

DHS-2.9.1.1 Requirement:

The organization shall develop, disseminate, and periodically review/update:

1. A formal, documented, AMI system information and document management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
2. Formal, documented procedures to facilitate the implementation of the AMI system information and document management policy and associated system maintenance controls.

DHS-2.9.1.2 Supplemental Guidance:

The organization should ensure that the AMI system information and document management policy and procedures are consistent with applicable asset owner, federal, state, and municipal laws, directives, policies, regulations, standards, and guidance. The AMI system information and document management policy can be included as part of the asset owner's general information security policy for the organization. System information and document management procedures can be developed for the security program in general, and for a particular AMI component, when required.

DHS-2.9.1.3 Requirement Enhancements:

None.

DSH-2.9.1.4 Rationale

Uncontrolled access to information concerning electrical consumption, billing, and other aspects of utility operations exposes the utility and its customers to potential fraud, theft, and other kinds of larceny and may result in violations of laws for privacy and other, similar statutes. Policies for document management are necessary to protect from these kinds of error and misuse.

DHS-2.9.2 Information and Document Retention

DHS-2.9.2.1 Requirement:

The organization shall manage AMI components related data, including establishing retention policies and procedures for both electronic and paper data, and shall manage access to the data based on formally assigned roles and responsibilities.

DHS-2.9.2.2 Supplemental Guidance:

The organization shall develop policies and procedures detailing the retention of company information. These procedures address retention/destruction issues for all applicable information media. Any legal or regulatory requirements are considered when developing these policies and procedures. Information associated with the development and execution of an AMI system is important, sensitive, and needs to be appropriately managed.

DHS-2.9.2.3 Requirement Enhancements:

The organization shall perform legal reviews of the retention policies to ensure compliance with all applicable laws and regulations.

DSH-2.9.2.4 Rationale

Document and data retention is essential for forensic investigations of system failure, to monitoring for fraud and misuse, and may be required to satisfy legal obligations.

DHS-2.9.3 Information Handling

DHS-2.9.3.1 Requirement:

Organization implemented policies and procedures detailing the handling of information should be developed and periodically reviewed and updated.

DHS-2.9.3.2 Supplemental Guidance:

Written policies and procedures detail access, sharing, copying, transmittal, distribution, and disposal or destruction of AMI system information. These policies or procedures include the periodic review of all information to ensure it is being properly handled. The organization shall protect information against unauthorized access, misuse, or corruption during transportation or transmission. The organization shall distribute or shares information on a need-to-know basis and considers legal and regulatory requirements when developing these policies and procedures.

DHS-2.9.3.3 Requirement Enhancements:

None.

DSH-2.9.3.4 Rationale

Accidental and intentional misuse of data, including public dissemination, illicit reproduction, and destruction, often occur before information is recorded in a managed document. Clear and effective policies for handling of all business and operational information are therefore essential precursor to effective document management and retention policies.

DHS-2.9.4 Information Classification

DHS-2.9.4.1 Requirement:

All information related to AMI components shall be classified to indicate the protection required commensurate with its sensitivity and consequence. Classification shall be done in accordance with relevant industry standards.

DHS-2.9.4.2 Supplemental Guidance:

It is recommended that a minimum of three levels of classification be defined for information related to AMI components to indicate the protection required commensurate with its sensitivity and consequence. These levels may be company proprietary, restricted, or public, indicating the need, priority, and level of protection required for that information. These information classification levels provide guidance for access and control to include sharing, copying, transmittal, destruction and distribution appropriate for the level of protection required.

DHS-2.9.4.3 Requirement Enhancements:

None.

DSH-2.9.4.4 Rationale

Blanket policies for information handling are not effective. Separation of information into protection categories, such as ‘unrestricted’, ‘confidential’, ‘secret’, and ‘top secret’, is therefore a necessary part of implementable policies for information and document management.

DHS-2.9.5 Information Exchange

DHS-2.9.5.1 Requirement:

Formal contractual and confidentiality agreements shall be established for the exchange of information and software between the organization and external parties.

DHS-2.9.5.2 Supplemental Guidance:

When it is necessary for the AMI components to communicate information to another organization or external party system, the operators need to mutually develop a formal contractual and confidentiality agreement and use a secure method of communication.

These formal exchange policies, procedures, and security controls need to be in place to protect the exchange of information through the use of all types of communication facilities.

DHS-2.9.5.3 Requirement Enhancements:

If a specific component needs to communicate with another component outside the AMI system network, communications shall be limited to only the components that need to communicate. All other ports and routes shall to be locked down or disabled.

DSH-2.9.5.4 Rationale

Legally binding contracts protect the provider and recipient of information from its deliberate and unintentional misuses. By including in these contracts specific policies and procedures for handling data, both parties will understand the expected level of protection for the exchanged data and acceptable mechanisms for implementing that protection.

DHS-2.9.6 Information and Document Classification

DHS-2.9.6.1 Requirement:

The organization shall develop 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 various components of AMI system

DHS-2.9.6.2 Supplemental Guidance:

Companies use both comprehensive information and document management policies for their cyber security management system. Inherent in this is an information classification system that allows information assets to receive the appropriate level of protection. The organization defines information classification levels (e.g., restricted, classified, general, etc.) for access and control to include sharing, copying, transmittal, and distribution appropriate for the level of protection required. The organization also classifies all information (i.e., AMI system design information, network diagrams, process programs, vulnerability assessments, etc.) to indicate the need, priority, and level of protection required commensurate with its sensitivity and consequence.

DHS-2.9.6.3 Requirement Enhancements:

The organization periodically reviews information that requires special control or handling to determine whether such special handling is still required.

DSH-2.9.6.4 Rationale

Clear, consistent policies for assigning classification levels to information are necessary for adequate protection of sensitive data. Haphazard, inconsistent assignment of classification levels will render useless all policies which require this classification by eroding confidence in effectiveness of those policies.

DHS-2.9.7 Information and Document Retrieval

DHS-2.9.7.1 Requirement:

The organization shall develop policies and procedures that provide details of the retrieval of written and electronic records, equipment, and other media for components of the AMI system in the overall information and document management policy.

DHS-2.9.7.2 Supplemental Guidance:

Any legal or regulatory requirements shall be considered when developing these policies and procedures.

DHS-2.9.7.3 Requirement Enhancements:

The organization shall employ appropriate measures to ensure long-term records information can be retrieved (i.e., converting the data to a newer format, retaining older equipment that can read the data, etc.).

DSH-2.9.7.4 Rationale

Information stored for a long period of time (one or more years) is prone to loss by antiquation of storage technology (file formats and storage media in particular), degradation of storage media, and inadequate retrieval mechanisms. Procedures for maintaining the availability of long term records are therefore an essential part of all document retention policies.

DHS-2.9.8 Information and Document Destruction

DHS-2.9.8.1 Requirement:

The organization shall develop policies and procedures detailing the destruction and disposal of written and electronic records, equipment, and other media in the overall information and document management policy.

DHS-2.9.8.2 Supplemental Guidance:

This also includes the method of disposal, such as shredding of paper records, erasing of disks or other electronic media, or physical destruction. All legal or regulatory requirements need to be considered when developing these policies and procedures.

DHS-2.9.8.3 Requirement Enhancements:

None.

DSH-2.9.8.4 Rationale

Sensitive information that is discarded without due consideration will be available to external parties for their use and misuse. Appropriate methods of disposal shall be practiced to avoid leaking information and to ensure that all legal requirements pertaining to the protection of data are met.

DHS-2.9.9 Information and Document Management Review

DHS-2.9.9.1 Requirement:

The organization shall perform periodic reviews of compliance with the AMI system information and document security management policy to ensure compliance with any laws and regulatory requirements. The organization shall regularly review compliance in the information and document management security policy.

DHS-2.9.9.2 Supplemental Guidance:

The compliance review procedure needs to consider all legal and regulatory documentation requirements applicable to the AMI system.

DHS-2.9.9.3 Requirement Enhancements:

None.

DSH-2.9.9.4 Rationale

Policies are only effective if they are properly applied. Periodic reviews of both the policies and their application are necessary to sustain their relevance to business operations.

AMISP-2.9.1 Automated Marking

AMISP-2.9.1.1 Requirement:

The components of AMI system shall automatically mark any external data output (physical/paper output) using standard naming conventions to identify any special dissemination, handling, or distribution instructions.

AMISP-2.9.1.2 Supplemental Guidance:

Automated marking refers to markings employed on external media (e.g., hardcopy documents output from the AMI components).

AMISP-2.9.1.3 Requirement Enhancements:

None.

AMISP-2.9.1.4 Rationale

Documents shall be appropriately marked to ensure handling as required by document management and retention policies

DHS-2.10 System Development and Maintenance

DHS-2.10.1 System Maintenance Policy and Procedures

DHS-2.10.1.1 Requirement:

The organization shall develop, disseminate, and regularly review and update:

1. A documented policy for maintenance of all components of the AMI system. These documents address purpose, scope, roles, responsibilities, coordination among organizational entities, and compliance testing.
2. Documented procedures for implementing the maintenance policy and associated system maintenance controls.

DHS-2.10.1.2 Supplemental Guidance:

The organization should ensure that the maintenance policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The maintenance policy can be included as part of the general information security policy for the organization. Maintenance policies and procedures can be developed for the security program in general and for particular components of the AMI system when required.

DHS-2.10.1.3 Requirement Enhancements:

None.

DHS-2.10.1.4 Rationale:

Appropriate system maintenance is vital to the smooth and consistent operation. Written policies and procedures are more likely to be consistently followed, and provide a measure to check against.

DHS-2.10.2 Legacy System Upgrades

DHS-2.10.2.1 Requirement:

The organization shall develop policies and procedures to upgrade all legacy components of the AMI system to include security mitigating measures needed to bring all elements of the AMI system into compliance with current security requirements commensurate with the organization's risk tolerance for those components.

DHS-2.10.2.2 Supplemental Guidance:

Legacy systems are those components currently in place as part of a working AMI system. 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 security configuration of legacy components and updates or replaces hardware and software as required.

DHS-2.10.2.3 Requirement Enhancements:

None.

DHS-2.10.2.4 Rationale:

Electric reliability and control depend upon restricting control to authorized actors in a system. AMI systems have many components which are very easy for attackers to touch and potentially control. Failing to continually maintain appropriate security in an AMI system leaves it open to outsider control.

DHS-2.10.3 System Monitoring and Evaluation

DHS-2.10.3.1 Requirement:

The organization shall regularly evaluate all components of the AMI system for security vulnerabilities and for compliance with its maintenance and security policies. All components of the AMI system shall be updated or replaced to address identified vulnerabilities or non-compliance issues in accordance with the maintenance policy and procedures.

DHS-2.10.3.2 Supplemental Guidance:

The frequency of evaluations is based on the organization's risk mitigation policy. Changing security requirements and discovery of vulnerabilities necessitate a review. These reviews should be carefully planned and documented in accordance with the organization’s maintenance policies and procedures.

DHS-2.10.3.3 Requirement Enhancements:

None.

DHS-2.10.3.4 Rationale:

No system is impervious to attack. The goal of cyber-security is to dissuade and slow attackers, identify successful attacks and effectively respond and handle security incidents. Monitoring systems throughout the AMI infrastructure can be vital to identifying that an attack has occurred.

DHS-2.10.4 Backup and Recovery

DHS-2.10.4.1 Requirement:

The organization shall secure backups of critical software, applications, and data for all components of the AMI system. The organization shall backup all data and applications needed to replace failed components within a reasonable period of time in accordance with organizational policies and as required to satisfy regulatory requirements. Backups shall be physically separated from the operational components.

DHS-2.10.4.2 Supplemental Guidance:

AMI components may be compromised due to an incident or disaster. A copy of essential software and data should be made, updated regularly, and stored in a secure environment for later use to restore the system to normal operations.

DHS-2.10.4.3 Requirement Enhancements:

None.

DHS-2.10.4.4 Rationale:

When systems fail or are compromised, successful backups are vital for restoring operations in a timely fashion. Those same system backups, however, represent significant risk for the security of the organization if not handled securely. Passwords, encryption keys, and other vital data are all available if someone is able to get ahold of them.

DHS-2.10.5 Unplanned System Maintenance

DHS-2.10.5.1 Requirement:

The organization shall review and follow security requirements before undertaking any unplanned maintenance on any component of the AMI system. Unplanned maintenance shall be documented and include the following:

1. The date and time of maintenance;
2. The name of the individual(s) performing the maintenance;
3. A description of the maintenance performed; If physical access or modification is required, also document the following:
    - The name of the escort, if necessary;
    - A list of equipment removed or replaced (including identification numbers, if applicable).

DHS-2.10.5.2 Supplemental Guidance:

Unplanned maintenance is required to support system operation in the event of system/component malfunction or failure. Security requirements necessitate that all unplanned maintenance activities use approved contingency plans and document all actions taken to restore operability to the system.

DHS-2.10.5.3 Requirement Enhancements:

The organization documents the decision and justification should unplanned maintenance not be performed after the identification of a security vulnerability.

DHS-2.10.5.4 Rationale:

Untracked changes can lead to poor decision-making when dealing with systems impacted.

Without official policy of change-tracking, potentially malicious changes may go unnoticed.

DHS-2.10.6 Periodic System Maintenance

DHS-2.10.6.1 Requirement:

The organization schedules, performs, and documents routine preventive and regular maintenance for all components of the AMI system in accordance with manufacturer or vendor specifications and/or organizational policies and procedures. The organization also explicitly approves the removal of the system or system components from organizational facilities for offsite maintenance or repairs, sanitizes the equipment to remove all information from associated media prior to removal from organizational facilities for offsite maintenance or repairs, and checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions

DHS-2.10.6.2 Supplemental Guidance:

Hardware maintenance includes planned replacement of functional equipment (e.g., deployment of new routers). Software maintenance (e.g., patches), like hardware maintenance, requires taking components off-line for some period of time. All maintenance should be approved by the appropriate organization official(s) and planned to avoid significant impact on operations. After maintenance is performed, the organization checks the security features to ensure that they are still functioning properly.

DHS-2.10.6.3 Requirement Enhancements:

1. The organization keeps a maintenance record for the system that includes the date and time of maintenance, the name of the individual(s) performing the maintenance, the name of the escort (if necessary), a description of the

maintenance performed, and a list of equipment removed or replaced (including identification numbers, if applicable).

2. The organization employs automated mechanisms to schedule and conduct maintenance as required and to create up-to-date, accurate, complete, and available records of all maintenance actions, both needed and completed.
3. Before disposal of equipment, all critical/sensitive information (e.g., keys) shall be removed using approved procedures.

DHS-2.10.6.4 Rationale:

Untracked changes can lead to poor decision-making when dealing with systems impacted.

Without official policy of change-tracking, potentially malicious changes may go unnoticed.

Proper disposal of information-storing system components can lead to vital access control or security information being available to dumpster-diving or second-hand hardware stores.

AMISP-2.10.1 Field Tools

AMISP-2.10.1.1 Requirement:

The organization shall approve, manage, protect, and monitor the use of field tools and maintains the integrity of these tools on an ongoing basis.

AMISP-2.10.1.2 Supplemental Guidance:

The intent of this requirement is to address hardware and software connected to component of the AMI system for diagnostics and repairs (e.g., a hardware or software packet sniffer introduced for a particular maintenance activity). Field tools include, for example, diagnostic and test equipment used to conduct maintenance on the network's software or hardware. Hardware and/or software components that may support maintenance yet are a part of the system (e.g., the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch) are not covered by this requirement.

AMISP-2.10.1.3 Requirement Enhancements:

1. The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications
2. The organization shall check all media containing diagnostic and test programs for malicious code before the media are used in the AMI system.
3. The organization shall check all field tools that can retain information so that no sensitive information is written on the equipment or the equipment is appropriately sanitized before release; if the equipment cannot be sanitized, the

equipment remains within the facility or is destroyed unless an appropriate organization official explicitly authorizes an exception.

4. The organization shall secure all field tools through the use of appropriate technology including, but not limited to, full-volume encryption and requiring two-factor authentication to logon to devices containing the field tools. Additional measures shall be implemented in order to ensure that the data contained within the field tools is secured appropriately.

AMISP-2.10.1.4 Rationale:

Many field tools represent significant access and control over AMI systems and should be carefully protected.

DHS-2.10.8 Maintenance Personnel

DHS-2.10.8.1 Requirement:

The organization shall document authorization and approval policies and procedures and maintains a list of personnel authorized to perform maintenance on the AMI System. Only authorized and qualified organization or vendor personnel perform maintenance.

DHS-2.10.8.2 Supplemental Guidance:

Maintenance personnel should have appropriate access authorization when maintenance activities allow access to organizational information that could result in a future compromise of availability, integrity, or confidentiality. When maintenance personnel do not have required access authorizations, organizational personnel with appropriate access authorizations supervise maintenance personnel during the performance of maintenance activities.

DHS-2.10.8.3 Requirement Enhancements:

None.

DHS-2.10.8.4 Rationale:

Tracking parties authorized to perform maintenance on each system helps avoid social-engineering attacks and or otherwise undue access to the systems.

Maintaining a list of authorization provides a discrete scope of responsibility for each given system. These people are the first ones to answer for issues with a system.

DHS-2.10.9 Remote Maintenance

DHS-2.10.9.1 Requirement:

The organization shall authorize, manage, and monitor remotely executed maintenance and diagnostic activities on all components of the AMI system. When remote

maintenance is completed, the organization or AMI component shall terminate all sessions and remote connections invoked in the performance of that activity.

DHS-2.10.9.2 Supplemental Guidance:

Remote maintenance and diagnostic activities are conducted by individuals communicating through an external, non-organization-controlled network (e.g., the Internet).

DHS-2.10.9.3 Requirement Enhancements:

1. The use of remote maintenance and diagnostic tools shall be consistent with organizational policy and documented in the security plan.
2. The organization shall maintain records for all remote maintenance and diagnostic activities.
3. The organization shall audit all remote maintenance and diagnostic sessions and appropriate organizational personnel review the maintenance records of the remote sessions.
4. The organization shall address the installation and use of remote maintenance and diagnostic links in the security plan.

DHS-2.10.9.4 Rationale:

Remote access to AMI systems represents a provision of control to an external party. Strict management and validation of termination of such access is vital for maintaining control over the overall AMI system.

DHS-2.12 Incident Response

DHS-2.12.1 Incident Response Policy and Procedures

DHS-2.12.1.1 Requirement:

The organization shall develop, disseminate, and periodically review and update:

1. A documented incident response policy that addresses purpose, scope, roles, responsibilities, coordination among organizational entities, and compliance; and
2. Documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

DHS-2.12.1.2 Supplemental Guidance:

The organization should ensure the incident response policy and procedures are consistent with applicable laws, directives, policies, regulations, standards, and guidance.

DHS-2.12.1.3 Requirement Enhancements:

None.

DHS-2.12.1.4 Rationale:

Incident response policy and procedures are important in many different ways.

During a cyber-security incident tension levels are high, communications paths may be hindered, and lack of preparation can prove hazardous. During these times, documented procedures and policies which have been studied and practiced can help to avoid mistakes, embody a certain level of organizational buy-in, and allow for vital incident response preparation involving both architectural design as well as training for staff.

DHS-2.12.2 Continuity of Operations Plan

DHS-2.12.2.1 Requirement:

The organization shall develop and implement a continuity of operations plan dealing with the overall issue of maintaining or re-establishing operation of the AMI system in case of an undesirable interruption. The plan addresses roles, responsibilities, assigned individuals with contact information, and activities associated with restoring system operations after a disruption or failure. Designated officials within the organization review and approve the continuity of operations plan.

DHS-2.12.2.2 Supplemental Guidance:

A continuity of operations plan addresses both business continuity planning and recovery of all vital AMI system operations.

DHS-2.12.2.3 Requirement Enhancements:

Following a disruption, the organization executes its incident response policies and procedures to place the system in a safe configuration and initiates the necessary notifications to regulatory authorities and initiates a root cause analysis for the event and submits any findings from the analysis to the organizations corrective action program.

DHS-2.12.2.4 Rationale:

Systems fail, mistakes occur. Continuity of Operations Plans allow for the expedient recovery from such situations. Creating such plans often bring weaknesses to light, allowing an organization to design additional safe-guards into the AMI system necessary for such recovery.

DHS-2.12.3 Continuity of Operations Roles and Responsibilities

DHS-2.12.3.1 Requirement:

The organization's continuity of operations plan shall define and communicate the specific roles and responsibilities for each part of the plan in relation to various types of disruptions to the operation of the AMI system.

DHS-2.12.3.2 Supplemental Guidance:

The continuity of operations plan defines the roles and responsibilities of the various employees and contractors in the event of a significant incident. The plans identify responsible personnel to lead the recovery and response effort if an incident occurs.

DHS-2.12.3.3 Requirement Enhancements:

None.

DHS-2.12.3.4 Rationale:

Specific roles and responsibilities within continuity plans allow for many of the confusing decisions to be made before an incident occurs. This clarification can ease the process and better focus the organization when recovering from a disruption.

AMISP-2.12.1 Incident Response Training

AMISP-2.12.1.1 Requirement:

The organization shall train personnel in their continuity of operations plan roles and responsibilities with respect to the AMI system. The organization shall provides refresher training annually. The training covers employees, contractors, and stakeholders in the implementation of the continuity of operations plan.

AMISP-2.12.1.2 Supplemental Guidance:

None.

AMISP-2.12.1.3 Requirement Enhancements:

Incident response retraining shall include the annual dissemination of information concerning the organizations incident response plan to utility customers.

AMISP-2.12.1.4 Rationale:

Training allows individuals to understand their part of the team and reduce mistakes and miscommunications which are frequent during incident response.

DHS-2.12.5 Continuity of Operations Plan Testing

DHS-2.12.5.1 Requirement:

The organization shall test the continuity of operations plan to determine its effectiveness and documents the results. Appropriate officials within the organization shall review the documented test results and initiate corrective actions if necessary. The organization shall test the continuity of operations plan for the AMI 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.

DHS-2.12.5.2 Supplemental Guidance:

Customers and utility operators need to be notified when testing is scheduled and informed as to how it will be conducted. There are several methods for testing and/or exercising continuity of operations plans to identify potential weaknesses (e.g., full-scale business continuity plan testing, functional/tabletop exercises, etc.).

DHS-2.12.5.3 Rationale:

The best laid plans fail. Periodic testing of continuity plans can identify weaknesses in design and implementation within a controlled situation when all staff are available. Changes to the plans or procedures during these exercises can limit the impact of a real incident or outage.

DHS-2.12.5.3 Requirement Enhancements:

The organization shall maintain a list of incident response activities and mitigations for the utility and its customers in accordance with the provisions of the organization incident response policy and procedures.

Following the preparation of the various plans, a schedule shall be developed to review and test each plan and ensure that each still meets the objectives.

Utility customers are notified of tests that could affect electrical service.

AMISP-2.12.2 Continuity of Operations Plan Update

AMISP-2.12.2.1 Requirement:

The organization shall review the continuity of operations plan for the AMI system at least annually and updates the plan to address system, organizational, and technology changes or problems encountered during plan implementation, execution, or testing.

AMISP-2.12.2.2 Supplemental Guidance:

Organizational changes include changes in mission, functions, or business processes supported by the AMI system. The organization should communicate the changes to appropriate organizational elements responsible for related plans.

AMISP-2.12.2.3 Requirement Enhancements:

Electrical customers will be notified immediately of changes to the plan that may affect them in the event of a contingency or otherwise.

AMISP-2.12.2.4 Rationale:

Even the most static environments change over time. In order to maintain reliability and control, the continuity plans shall be periodically reviewed and updated.

DHS-2.14 System and Information Integrity

Maintaining an AMI 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 AMI system flaws. Controls exist for malicious code detection, spam protection, and intrusion detection tools and techniques. Also provided are controls for receiving security alerts and advisories and the verification of security functions on the AMI system. In addition, there are controls within this family to 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.

DHS-2.14.1 System and Information Integrity Policy and Procedures

DHS-2.14.1.1 Requirement:

The organization shall develop, disseminate, and periodically review and update:

1. Documented, system and control integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
2. Documented procedures to facilitate the implementation, ongoing maintenance, and support of the AMI system and information integrity policy and associated system and information integrity controls.

DHS-2.14.1.2 Supplemental Guidance:

The system and information integrity policy should be included as part of the general control security policy for the organization. System and information integrity procedures should be developed for the security program in general, and for a particular AMI component, when required.

DHS-2.14.1.3 Requirement Enhancements:

The organization shall ensure the system and information integrity policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance.

DHS-2.14.1.4 Rationale:

Comprehensive system protection, timely response to newly discovered vulnerabilities, and improvements to security based on operational experience cannot be achieved without orderly, well-understood procedures and policies to coordinate and direct security initiatives in all parts of the organization. Regular reviews and updates of policies and procedures are therefore needed to ensure continuing relevance to business operations.

DHS-2.14.2 Flaw Remediation

DHS-2.14.2.1 Requirement:

The organization shall identify, report, and remediate AMI system vulnerabilities (per organizational, legal, and/or regulatory policies).

The organization shall identify AMI systems and system components containing software affected by recently announced vulnerabilities (and potential vulnerabilities resulting from those flaws).

The organization (or the software developer/vendor for software developed and maintained by a vendor/contractor) shall promptly evaluate newly released security-relevant patches, service packs, and hot fixes and tests them for effectiveness and potential impacts on the organization's AMI system before installation.

DHS-2.14.2.2 Supplemental Guidance:

Proprietary software can be found in either commercial/government off-the-shelf component products or in custom-developed applications. Vulnerabilities discovered during security assessments, continual monitoring, or under incident response activities also need to be addressed expeditiously. It is generally not recommended to shut down and restart AMI system components when an anomaly is identified.

DHS-2.14.2.3 Requirement Enhancements:

1. The organization shall centrally manage the vulnerability remediation process and installs updates automatically. Organizations shall consider the risk of employing automated flaw remediation processes on an AMI system;
2. The use of automated vulnerability remediation processes shall not degrade the operational performance of the AMI system;
3. The organization shall employ automated mechanisms to periodically and upon demand determine the state of AMI system components with regard to vulnerability remediation.

DHS-2.14.2.4 Rationale:

Timely identification and remediation of discovered vulnerabilities is the only way to ensure that the system remains secure in an evolving threat environment. The need for

protection from malicious actors and software failures shall be balanced against the risk of inadvertently introducing new failure modes into the system. Centrally managed flaw remediation ensures a single clearing house where informed decisions can be made about the when and how to remediate new vulnerabilities.

DHS-2.14.3 Malicious Code Protection

DHS-2.14.3.1 Requirement:

The AMI system shall employ malicious code protection.

From a system perspective, malicious code protection mechanisms shall be deployed in such a manner as to limit the impact of the attack to a small geographical area prior to detection and eradication. These include critical entry and exit points between Wide Area Networks (WAN), Neighborhood Area Networks (NAN), and in-premise networks.

DHS-2.14.3.2 Supplemental Guidance:

Malicious code protection mechanisms are central to the AMI system design to control the flow of information within the interconnected elements of the system and to detect and eradicate malicious code.

One challenge of an AMI system design is that the field deployed devices are typically not suitable for traditional third party malicious code protection mechanisms. This combined with very little or no physical security warrants that emphasis be placed on the risk associated with these widely dispersed assets. For the AMI meters in particular, the Home Area Network (HAN) interface represents and entry point not only into the device but into the utility's Neighborhood Area Network (NAN) as well. The AMI meter should ensure that no malicious code can pass from the consumer's HAN to the utility's NAN. The AMI meter should also protect the consumer's HAN equipment from any attack which attempts to propagate malicious code utilizing the utility's NAN.

Field tools represent a potentially higher risk due to their portability and likelihood of being connected to numerous networks. If not properly secured and controlled, they can be a mechanism to bypass security controls and allow malicious code to be transported from one security zone to another.

In all cases, care should be taken if automated response mechanisms are deployed so that receipt of false positives from the malicious code protection mechanisms does not adversely affect the availability of the AMI system.

DHS-2.14.3.3 Requirement Enhancements:

1. The use of mechanisms to centrally manage malicious code protection shall not interfere with the reliable operation of the AMI system.

2. All signature files and definitions for malicious code detection mechanisms used within the AMI system shall be updated automatically from a centralized managed trusted source.
3. Centralized configuration management and change control shall be employed for all AMI system assets.
4. Periodic and automatic auditing/verification of configuration (programming parameters, firmware and revision level, etc.) shall be performed for all AMI system assets.
5. All detection of and actions taken within the AMI system to respond to malicious code shall be logged to a centralized repository.
6. Intrusion detection (logging) shall be installed within each Neighborhood Area Network (NAN) network segment with event monitoring / event response and subsequent prevent for incoming and outgoing network traffic, including anti-virus, anti-spyware and signature and anomaly-based traffic monitors.
7. Access Control Lists (ACL) shall be employed at all points which bridge Neighborhood Area Network (NAN) segments to Wide Area Networks (WAN) to limit incoming and outgoing connections to only those necessary to support the AMI system.
8. Dynamic packet filtering shall be employed at all points which bridge Neighborhood Area Network (NAN) segments and Wide Area Networks (WAN).
9. The transfer of executable files through the perimeters of the Neighborhood Area Network (NAN) and the Wide Area Network (WAN) shall be restricted.
10. All components of the AMI system or any device connected to the AMI network shall employ host hardening, including patch application and security-minded configurations of the operating system (OS), browsers, and other network-aware software. All components of the AMI system or any device connected to the AMI network shall employ integrity checking mechanisms for firmware/software.
11. All firmware/software shall be scanned prior to loading on any component of the AMI system or device connected to the AMI network.
12. The authenticity of all firmware/software shall be verified prior to loading on any component of the AMI system or device connected to the AMI network.
13. All AMI components shall be verified to have the proper software revisions and patches prior to being allowed full operation within the AMI network.
14. The AMI meter or gateway device shall not allow uploading of any executable code from the consumer's HAN.
15. Field tools shall have additional control applied as follows:

1. Security updates from the manufacturer of the appropriate operating system, and/or application software, shall be kept current (e.g., patched and updated) on all field tools.
2. Where applicable field tools shall employ firewall software or hardware to aid in the prevention of malicious code attacks/infections.
3. Field tools shall employ host hardening, including patch application and security-minded configurations of the operating system (OS), browsers, and other network-aware software.
4. Field tools shall utilize anti-virus, anti-spam, and anti-spyware software.
5. Field tools shall scan removable media devices for malicious code before accessing any data on the media.
6. Field tools shall scan email attachments and shared files of unknown integrity for malicious code before they are opened or accessed.
7. The field tool shall utilize a restricted operating system which only allows execution of known and signed code/applications.

DHS-2.14.3.4 Rationale:

These are technical best practices adopted throughout industry for networks and computers used for business IT purposes. Failure to apply any of these best practices exposes the violator to demonstrable risk from malicious agents.

DHS-2.14.4 System Monitoring Tools and Techniques

DHS-2.14.4.1 Requirement:

All components of the AMI system shall detect, log and report all security events and system activities to the AMI management system.

DHS-2.14.4.2 Supplemental Guidance:

Effective monitoring, logging, and alerting of security events and anomalies requires that all components of the AMI system should be able to generate appropriate logs corresponding to predefined security events and anomalies.

Including accurate and relevant information in log files is essential. In general, all logs from AMI system components should answer the five basic questions of; Who, What, Where, When, and How. When determining the actions of reading, writing, deleting, and modification of data, it should be possible to determine the process, who owns it, when it was initiated, where the action occurred, and why the process ran. Additionally, all administrative, authentication, authorization, and communication events associated with any AMI system component should be logged and reported.

One challenge when considering an attack on a field-deployed AMI component is that the logging and reporting capability of the component may have be compromised and/or disabled by the attacker. If the monitoring system is only equipped to alert based on logs/report which are sent by the end devices, an attack may go undetected for some period of time.

AMI components should support open log formats, such as SYSLOG format (RFC 3164).

DHS-2.14.4.3 Requirement Enhancements:

1. The monitoring and logging function shall not adversely impact the operational performance of the AMI system or component.
2. Logs generated by AMI system components shall conform to all applicable recommendations outlined in NIST SP800-92, Guide to Computer Security Log Management.
3. The AMI system component shall provide an authentication mechanism for the logs.
4. The AMI system component shall provide a mechanism by which missing logs are detected.
5. The AMI system component shall be capable of storing a sufficient number of security events in the components buffer to support the system-wide monitoring function.

DHS-2.14.4.4 Rationale:

Logs of system events are essential for forensics following an attack or system error and for the detection and identification of malicious activity and system errors.

DHS-2.14.5 Security Alerts and Advisories

DHS-2.14.5.1 Requirement:

The organization:

1. Receives AMI 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.

DHS-2.14.5.2 Supplemental Guidance:

The organization documents the types of actions to be taken in response to security alerts and advisories.

DHS-2.14.5.3 Requirement Enhancements:

The organization shall employ automated mechanisms to make security alert and advisory information available throughout the organization as needed.

The organization also shall maintain contact with special interest groups (e.g., information security forums) that:

1. Facilitate sharing of security-related information (e.g., threats, vulnerabilities, and latest security technologies);
2. Provide access to advice from security professionals;
3. Improve knowledge of security best practices.

DHS-2.14.5.4 Rationale:

To maintain a relevant security posture, it is necessary to be aware of the security landscape as it evolves. Receiving and acting on relevant computer security advisories and alerts is therefore a necessary part of maintaining effective defenses.

AMISP-2.14.1 Security Functionality Verification

AMISP-2.14.1.1 Requirement:

All components of the AMI system shall employ controls which independently and in concert with the AMI management system verify that that all security functions within the component are in an online/active state. This shall be done upon component and system startup and restart; upon command by a user with appropriate privilege; periodically; and/or at defined time periods.

AMISP-2.14.1.2 Supplemental Guidance:

The AMI management system should be designed with security in mind, such that AMI components will require proper operation of security functionality to function.

In addition to processing requests initiated by the AMI management system, the AMI system components shall also be able to perform basic automated self-tests independent of the AMI management system. Because of wide geographic deployment and limited physical security of the field deployed AMI components, verification of the proper operation of the security functionality is essential for these components.

AMISP-2.14.1.3 Requirement Enhancements:

1. All AMI system components shall be capable of periodically performing automated self-test of the security functions at predefined intervals.
    1. Any failure of the component self-test shall result in a security event being logged and reported to the appropriate logging system (for further details, see requirement "2.14.4 System Monitoring Tools and Techniques").

2. Any failure of the component self test shall result in the component transitioning to a safe state including:
    1. Inhibiting all control capabilities of the component.
    2. Inhibiting all communications initiated within the HAN to the NAN.
    3. Inhibiting all relaying/repeating functionality of the component.

AMISP-2.14.1.4 Rationale:

System components without functioning security features are likely to have been compromised or to be compromised in the near future. These devices cannot be expected to operate properly and should therefore be removed from service.

DHS-2.14.7 Software and Information Integrity

DHS-2.14.7.1 Requirement:

The AMI system shall monitor and detect unauthorized changes to software, firmware, and data.

DHS-2.14.7.2 Supplemental Guidance:

None.

DHS-2.14.7.3 Requirement Enhancements:

The organization shall employ integrity verification techniques on the AMI system to look for evidence of information tampering, errors, and/or omissions. The organization shall employ good software engineering practices with regard to commercial-off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and uses tools to automatically monitor the integrity of the IT systems, AMI components, and the applications they host.

Although automated tools can be risky for use in AMI system, the following can be considered as appropriate for the AMI system:

1. The organization shall reassess the integrity of software, firmware, and data by performing integrity scans of the AMI system;
2. The organization shall employ automated tools that provide notification to appropriate individuals upon discovering discrepancies during integrity verification;
3. The organization shall employ centrally managed integrity verification tools;
4. The use of integrity verification applications shall not adversely impact the operational performance of the AMI system.

DHS-2.14.7.4 Rationale:

System components that have undergone unexpected or unauthorized modifications are likely to have been compromised or to be malfunctioning. These components shall be detected and reported to the appropriate personnel for assessment and correction.

DHS-2.14.8 Unauthorized Communications Protection

DHS-2.14.8.1 Requirement:

The AMI system shall implement unauthorized communications (e.g. spam) protection.

DHS-2.14.8.2 Supplemental Guidance:

The organization uses the unauthorized communications protection mechanisms to detect and take appropriate action on unsolicited messages transported by electronic mail, electronic mail attachments, Internet access, or other common means. The organization considers using unauthorized communications protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another for workstations).

For an AMI system, the organization should minimize any use of and remove if possible any electronic messaging functions and services (e.g., electronic mail, Internet access). Due to differing operational characteristics between AMI systems and general IT systems, AMI systems do not generally employ spam protection mechanisms. Unusual traffic flow, such as during crisis situations, may be misinterpreted and caught as unauthorized communications, which can cause issues with the system and possible failure of the system.

DHS-2.14.8.3 Requirement Enhancements:

The organization shall employ unauthorized communications protection mechanisms at critical AMI system entry points (e.g., firewalls, electronic mail servers, remote-access servers) and at workstations, servers, and/or mobile computing devices on the network.

The organization shall centrally manage unauthorized communications protection mechanisms. The AMI system shall automatically update unauthorized communications protection mechanisms. Organizations consider the risk of employing mechanisms to centrally manage unauthorized communications protection on an AMI system. The use of mechanisms to centrally managed unauthorized communications protection shall not degrade the operational performance of the AMI system.

DHS-2.14.8.4 Rationale:

Unsolicited electronic messages are a well known venue for attacking computer systems. Where email, instant messaging, and other methods are used to send and receive information within the AMI system, detection and elimination of unsolicited messages is an important facet of system protection. Particularly vulnerable are field devices that may

acquire infections via the receipt of spam and pass these to the AMI network at a later time.

DHS-2.14.9 Information Input Restrictions

DHS-2.14.9.1 Requirement:

The organization shall implement security measures to restrict information input to the AMI system to authorized personnel only.

DHS-2.14.9.2 Supplemental Guidance:

Restrictions on personnel authorized to input information to the AMI system may extend beyond the typical access requirements employed by the system and include limitations based on specific operational or project responsibilities.

DHS-2.14.9.3 Requirement Enhancements:

None.

DHS-2.14.9.4 Rationale:

Manipulation of physical devices, such as connecting and disconnecting electrical power to a home or business, can damage electrical equipment and pose a threat to safety. Input to an AMI system that may alter its physical configuration must therefore be limited to personnel who routinely need to make such adjustments in the performance of their duties.

AMISP-2.14.2 Information Input Accuracy, Completeness, Validity, and Authenticity

AMISP-2.14.2.1 Requirement:

All AMI system components shall employ controls to check information for accuracy, completeness, validity, and authenticity.

AMISP-2.14.2.2 Supplemental Guidance:

The design of the AMI system component should consider all valid inputs during its operation. The AMI system component should filter all inputs and allow only those matching a predefined valid set to be processed by the internal hosted application(s). All other inputs not matching this predefined set should be rejected and logged.

AMISP-2.14.2.3 Requirement Enhancements:

None.

AMISP-2.14.2.4 Rationale:

Manipulation of physical devices, such as connecting and disconnecting electrical power to a home or business, can damage electrical equipment and pose a threat to safety. Input to an AMI system that may alter its physical configuration therefore deserves particular scrutiny.

DHS-2.14.11 Error Handling

DHS-2.14.11.1 Requirement:

All AMI system components shall employ controls to identify and handle error conditions in an expeditious manner without providing information that could be exploited by adversaries.

DHS-2.14.11.2 Supplemental Guidance:

The structure and content of error messages displayed by and transmitted from the AMI system components should to be carefully considered by the organization. These error messages should provide timely and useful information without providing potentially harmful information that could be exploited by adversaries. Detailed AMI system component error messages should be revealed only to authorized personnel (e.g., systems administrators, maintenance personnel).

The nature of the AMI system architecture makes it susceptible to observing messages displayed on components and monitoring messages transmitted between components. As such, this opens the risk of an attacker determining specific details about the system or its components by observing error messages on device displays or monitoring error messages transmitted from the field deployed AMI components. Such details can provide hackers important clues on potential flaws in the AMI components.

Risks associated with improper error handling are not limited to those which are transparent to the system operation. AMI system components should not be susceptible to security problems caused by improper error handling, such as:

1. Fail-open security check – The component should assume no access until proven otherwise. All security mechanisms should deny access until specifically granted, not grant access until denied, which is a common reason why fail open errors occur.
2. Impacts to component resources - Errors that can cause the component to crash or consume significant resources, effectively denying or reducing service to legitimate users.

DHS-2.14.11.3 Requirement Enhancements:

1. Error messages displayed by any field deployed AMI component should provide limited information so as not to disclose details of the internal systems operation. . The component shall provide the user with diagnostic information (e.g., data

validation errors), but should NOT provide developer level diagnostic/debug information. Detailed error messages should only be transmitted to the utilities designated logging server.

2. The AMI component shall not fail in an open condition (grant access unless specifically denied).

DHS-2.14.11.4 Rationale:

Detailed records of software failures (e.g., core dumps, names of missing link libraries, and other specific, technical information) are frequently used to find and exploit security holes. Restricting access to this type of information is therefore an important security practice. Secure coding practices that help prevent security breeches following a software error are a widely documented best practice that should be followed by organizations developing software for AMI components.

DHS-2.14.12 Information Output Handling and Retention

DHS-2.14.12.1 Requirement:

The organization shall handle and retain output from the AMI system in accordance with applicable laws, regulations, standards, and organizational policy, as well as operational requirements of the AMI system.

DHS-2.14.12.2 Supplemental Guidance:

None.

DHS-2.14.12.3 Requirement Enhancements:

None.

DHS-2.14.12.4 Rationale:

Output data produced by devices in the AMI system are an essential tool for forensic investigation of system failures and for the detection and mitigation of errors and malicious action. Retention of this data may also be required to satisfy legal obligations.

DHS-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 put into place to monitor access activities for inappropriate access attempts. 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 component, as a prerequisite for granting access to resources in an AMI system. Identification could use a password, a cryptographic token, or a biometric (e.g. fingerprint). Authentication is the challenge process to prove (validate) the identification provided. An example is using a fingerprint (identification) to access a computer via a biometric device (authentication). The biometric device authenticates the identity of the fingerprint.

DHS-2.15.1 Access Control Policy and Procedures

DHS-2.15.1.1 Requirement:

The organization shall develop, disseminate, and periodically review/update:

1. A formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
2. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

Access control policies and procedures for highly-critical management tasks shall specify strict security controls commensurate with the criticality of the task - including requirements for physical presence at a management console situated in a physically secure location, multiple levels of approval/authorization (by those with appropriate organizational roles), and strong multi-factor authentication and/or equivalent methods.

The organization shall ensure that access control policy and procedures are consistent with applicable laws, directives, policies, regulations, standards, and guidance.

DHS-2.15.1.2 Supplemental Guidance:

The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general, and for a particular AMI component, when required.

DHS-2.15.1.3 Requirement Enhancements:

It is recommended that the access control policy include the requirement that the HAN interface shall pass no control signals to the utility. Only informational signals may be passed on to the utility which shall base no control decisions on HAN-sourced communications without confirmation that the HAN-sourced information is authenticated and consistent with information provided from utility-owned devices within utility-controlled security domains (physical and logical). The utility shall have the ability to set the HAN interface to ignore (i.e., filter) non-authenticated HAN communications or communications from specific HAN-devices when it deems such communications to be a threat to security or safety.

DHS-2.15.1.4 Rationale:

A documented process for managing access rights is a well established, best practice and absence of such a policy exposes the AMI system to demonstrable risks. The specific guidance for the HAN network is appropriate because 1) it is not under the control of the utility and so shall be considered untrustworthy, and 2) by including the home owner's computers and, possibly, other network-enabled devices, the HAN and everything reachable from it is subjected to all the hazards of the Internet. Therefore, every point of entry into the AMI network via the HAN incurs significant risk.

DHS-2.15.2 Identification and Authentication Policy and Procedures

DHS-2.15.2.1 Requirement:

The organization shall develop, disseminate, and periodically review/update:

1. A formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for associated identification and authentication controls;
2. Formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

All communications between AMI components shall be authenticated. Any communications upon which critical management and control decisions are based shall be confirmed by multiple independent means (which may include "out-of-band" communications).

Any communication to be passed onto the utility by the HAN-interface shall be authenticated and non-control in nature.

The organization shall ensure the identification and authentication policy and procedures are consistent with applicable laws, directives, policies, regulations, standards, and guidance.

DHS-2.15.2.2 Supplemental Guidance:

The identification and authentication policy can be included as part of the general security policy for the organization. Identification and authentication procedures can be developed for the security program in general, and for a particular AMI system, when required.

DHS-2.15.2.3 Requirement Enhancements:

None.

DHS-2.15.2.4 Rationale:

Requiring authentication prior to accessing network or computer resources is an industry best practice. Once again, the HAN receives particular attention due the risk that it poses to the AMI system.

DHS-2.15.3 Account Management

DHS-2.15.3.1 Requirement:

The organization shall manage AMI system accounts, including authorizing, establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews AMI system accounts, policies, and procedures at least annually, with the frequency depending on criticality.

The organization shall identify authorized users of the AMI system and specifies access rights and privileges; i.e., access control list. The organization shall grant access to the AMI system based on:

1. A valid need-to-know/need-to-share basis that is determined by assigned official duties and that satisfies all personnel security criteria;
2. Intended system use. The organization shall require proper identification for requests to establish AMI system accounts and shall approve all such requests. The organization specifically authorizes and monitors the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts. The organization ensures that account managers for the AMI system are notified when users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers are also notified when users' AMI system usage or need-to-know/need-to-share changes. In cases where accounts are role-based, i.e., the workstation, hardware, and/or field devices define a user role, access to the AMI system includes physical security policies and procedures based on organization risk assessment. In cases where physical access to the workstation, hardware, and/or field devices predefines privileges, the organization shall implement physical security policies, and procedures based on organization risk assessment. Account management may include additional account types (e.g., role-based, device-based, attribute-based). The organization removes, disables, or otherwise secures default accounts (e.g., maintenance).
3. Default passwords are changed.

DHS-2.15.3.2 Supplemental Guidance:

Account management includes the identification of account types (i.e., individual, group, role-based, device-based, and system), establishment of conditions for group membership, and assignment of associated authorizations.

DHS-2.15.3.3 Requirement Enhancements:

1. The organization shall employ automated mechanisms when possible to support the management of AMI system accounts. Where automated mechanisms are unavailable account management functions shall be performed manually.
2. The AMI system shall automatically terminate temporary and emergency accounts after a defined time period for each type of account.
3. The AMI system shall automatically disable inactive accounts.
4. The organization shall employ automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals.

DHS-2.15.3.4 Rationale:

These guidelines conform to well established, best practices.

DHS-2.15.4 Identifier Management

DHS-2.15.4.1 Requirement:

The organization shall manage user identifiers by:

1. Uniquely identifying each user;
2. Verifying the identity of each user;
3. Receiving authorization to issue a user identifier from an appropriate organization official;
4. Ensuring that the user identifier is issued to the intended party;
5. Disabling user identifier after a pre-determined time period of inactivity;
6. Archiving user identifiers.

DHS-2.15.4.2 Supplemental Guidance:

All actions within an AMI system should be traceable to an individual user. Guest, Anonymous, and Group accounts should not be used. Administrative / Authorative accounts should not be used for normal operation. For administrative tasks, individual accounts should be used in conjunction with temporary rights elevation procedures that are localized to a specific task or similar logging access-control mechanism.

For some AMI components, the capability for immediate operator interaction is critical. Local emergency actions for the AMI system should not be significantly hampered by identification requirements. Access to these systems may be restricted by appropriate physical security mechanisms, and should cause immediate alerting of security personnel.

DHS-2.15.4.3 Requirement Enhancements:

Failure of identification system shall not fail to an open unprotected state. It shall fail to a protected, recoverable backup state.

DHS-2.15.4.4 Rationale:

These guidelines conform to well established, best practices excepting the requirement for unhampered access to components that are critical to emergency response. In these cases, the system owner shall weigh the risk of less stringent access controls against the risk posed by an accidental lockout.

DHS-2.15.5 Authenticator Management

DHS-2.15.5.1 Requirement:

The organization shall manage AMI system authenticators by:

1. Defining initial authenticator content criteria;
2. Establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators;
3. Changing default authenticators upon AMI system installation;
4. Changing/refreshing authenticators periodically.
5. All permissions associated with authenticators should be maintained at as low a level as possible so that, in case of compromise, an attacker's access would be limited (see DHS-2.15.9 Least Privilege)

DHS-2.15.5.2 Supplemental Guidance:

System authenticators include, for example, cryptographic tokens, PKI certificates, biometrics, passwords, and key cards.

Factory default authentication credentials are often well known, easily discoverable, present a great security risk and therefore should be changed.

DHS-2.15.5.3 Requirement Enhancements:

Users take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately.

Passwords shall not be embedded into tools, source code, scripts, aliases or shortcuts. Many AMI components and software are shipped with factory default authentication credentials to allow for initial installation and configuration.

For symmetric/password-based authentication, the AMI system:

1. Shall protect passwords from unauthorized disclosure and modification when stored or transmitted;
2. Shall prohibit passwords from being displayed when entered;
3. Shall enforce password minimum and maximum lifetime restrictions;
4. Shall prohibit password reuse for a specified number of generations.

For asymmetric/PKI-based authentication, the AMI system:

1. Shall validate certificates by constructing a certification path to an accepted trust anchor;
2. Shall enforce authorized access to and use of the corresponding private key;
3. Shall map the authenticated identity to the user account.
4. Shall restrict field tools password and keys life-span in case they are stolen.

DHS-2.15.5.4 Rationale:

These guidelines conform to well established, best practices.

AMISP-2.15.1 Supervision and Review

AMISP-2.15.1.1 Requirement:

The organization shall supervise and review the activities of users with respect to the enforcement and usage of AMI system access control. AMI components shall provide auditing capability specified in section DHS-2.16.

AMISP-2.15.1.2 Supplemental Guidance:

The extent of the audit record reviews is based on the impact level of the AMI system. For example, for low-impact systems it is not intended that security logs be reviewed frequently for every workstation but rather at central points such as a web proxy or email servers and when specific circumstances warrant review of other audit records.
This plan should also include who is responsible for patches and updates and how they are to occur.

AMISP-2.15.1.3 Requirement Enhancements:

The organization shall:

1. review audit records (e.g., user activity logs) for inappropriate activities in accordance with organizational procedures
2. investigate any unusual AMI system-related activities and periodically review changes to access authorizations.
3. review the activities of users with significant roles and responsibilities for the AMI system more frequently.

4. have in place policies and procedures that deal specifically with breaches in security, that detail specifically what actions are to occur to secure the breach and investigate any damage.
5. employ automated mechanisms to facilitate the review of user activities on the AMI system.

DHS-2.15.7 Access Enforcement

DHS-2.15.7.1 Requirement:

AMI components shall enforce assigned authorizations for controlling access to the system in accordance with applicable policy.

Access to AMI components that perform management functions (e.g. Field Tool) shall be tightly controlled. Interfaces of particular interest are AMI components that use a PC (or laptop) or mobile devices for interfacing with control functions.

DHS-2.15.7.2 Supplemental Guidance:

Access control policies (e.g., identity-based policies, role-based policies, rule-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 AMI system.

DHS-2.15.7.3 Requirement Enhancements:

The organization shall consider the implementation of a controlled, audited, and manual override of automated mechanisms in the event of emergencies or other serious events.

The functionality of field tools and other systems which perform managed services shall be limited to the bare minimum to perform the needed task. E-mail and web functions should be removed or limited to access only an approved list. Other applications not required to perform the functions shall be removed.

1. The AMI system shall restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel. Explicitly authorized personnel include, for example, AMI system operators, security administrators, system and network administrators, and other privileged users who have access to system control, monitoring, or administration functions. Access to privileged functions by privileged users may also be restricted based on components (e.g., remote terminal units and field devices).
2. The AMI system shall requires dual authorization, based on approved organization procedures, to privileged functions that have impacts on facility, human, and environmental safety. The utility shall develop and implement a procedure that can be executed in times of emergency for access to otherwise restricted passwords and keys

3. Access enforcement mechanisms shall not adversely impact the operational performance of the AMI system.
4. The meter IR port shall be protected from unauthorized access. Permit only the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks (see section DHS-2.15.9 "Least Privilege").
5. The meter ESI interface shall be protected from unauthorized access. Permit only the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks (see section DHS-2.15.9 "Least Privilege").
6. AMI field tool shall require access control to utilize the tool. Field service tool shall not save or store customer information, passwords, encryption key, or any other information that may compromise the AMI system or network.
7. The HAN interface shall prevent HAN-devices access to utility control functions.

DHS-2.15.7.4 Rationale:

Access controls are meaningless without enforcement at both the device and the organizational levels.

DHS-2.15.8 Separation of Duties

DHS-2.15.8.1 Requirement:

All AMI components shall enforce separation of duties through assigned access authorizations.

DHS-2.15.8.2 Supplemental Guidance:

All AMI components should contain appropriate divisions of responsibility and separate duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. Examples of separation of duties include 1) mission functions and distinct AMI system support functions are divided among different individuals/roles; 2) different individuals perform AMI system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and 3) security personnel who administer access control functions should not administer audit functions.

DHS-2.15.8.3 Requirement Enhancements:

Access control software shall be on the AMI system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion.

The organization shall establish appropriate divisions of responsibility and separate duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals.

DHS-2.15.8.4 Rationale:

Separation of duties helps limit the overall system impact when a single user account or component is compromised.

DHS-2.15.9 Least Privilege

DHS-2.15.9.1 Requirement:

All AMI components shall enforce the most restrictive set of rights/privileges or accesses to users or workstations (or processes acting on behalf of users) for the performance of specified tasks.

DHS-2.15.9.2 Supplemental Guidance:

None..

DHS-2.15.9.3 Requirement Enhancements:

All AMI components shall employ the concept of least privilege for all accounts, protocols, and services. Services and protocols shall not be run under root or administrator accounts.

DHS-2.15.9.4 Rationale:

When the concept of least privilege is applied to all user accounts, system accounts, and system services, the attack value of any single account or service is decreased.

DHS-2.15.10 User Identification and Authentication

DHS-2.15.10.1 Requirement:

All AMI components shall uniquely identify and authenticate users (or processes acting on behalf of users).

DHS-2.15.10.2 Supplemental Guidance:

In addition to identifying and authenticating users at the AMI system level (i.e., at system logon), identification and authentication mechanisms are employed at the application level, when necessary, to provide increased information security for the organization.

Where users function as a single group (e.g., control room operators), user identification and authentication may be role-based, group-based, or device-based. For some components of AMI system, the capability for immediate operator interaction is critical. The utility should develop and implement a procedure that can be executed in times of emergency for access to otherwise restricted passwords and keys. Access to these systems may be restricted by appropriate physical security mechanisms.

DHS-2.15.10.3 Requirement Enhancements:

Each user shall be uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance with security control.

Authentication of user identities shall be accomplished through the use of passwords, tokens, biometrics, or in the case of multi-factor authentication, some combination of these.

Remote user access to AMI system components shall only be enabled when necessary, approved, and protected.

DHS-2.15.10.4 Rationale:

User authentication is a common layer of defense and presents a hurtle that attackers shall overcome before gaining access to a system.

DHS-2.15.11 Permitted Actions without Identification or Authentication

DHS-2.15.11.1 Requirement:

The organization shall identify, document, and provide security justification for specific user actions that can be performed on the AMI system without identification or authentication.

DHS-2.15.11.2 Supplemental Guidance:

None.

DHS-2.15.11.3 Requirement Enhancements:

The use of anonymous accounts, public accounts, and guest accounts is prohibited.

The HAN interface should not permit any actions (including communications) without identification or authentication. AMI components that perform management services (e.g. Field Tool) shall not be permitted to perform any actions without identification or authentication.

DHS-2.15.11.4 Rationale:

Every action that is permitted without authentication can be easily leveraged by attackers, thus the number of unauthenticated actions should be severely limited or eliminated.

DHS-2.15.12 Device Identification and Authentication

DHS-2.15.12.1 Requirement:

The AMI system shall employ a mechanism to identify and authenticate specific components before establishing a connection. In particular, the WAN, NAN, and HAN

interfaces shall require strong device level authentication, as do components that perform management services (e.g. Field Tool).

DHS-2.15.12.2 Supplemental Guidance:

The strength of the device authentication mechanism is based on the security categorization of the AMI system. Automatic equipment identification may be considered as a means to authenticate connections.

DHS-2.15.12.3 Requirement Enhancements:

Field devices shall have the capability to support authentication mechanisms

DHS-2.15.12.4 Rationale:

Device authentication is a common layer of defense and presents a hurtle that attackers shall overcome before gaining access to a system. This also prevents attackers from gaining access to the AMI system by spoofing existing devices.

DHS-2.15.13 Authenticator Feedback

DHS-2.15.13.1 Requirement:

The authentication mechanisms in the AMI component/system shall obfuscate feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. This applies to authentication by one component to another as well as by individuals.

DHS-2.15.13.2 Supplemental Guidance:

The feedback from the AMI component/system does not provide information that would allow an unauthorized user to compromise the authentication mechanism.

Authentication mechanisms should not provide differences which indicate whether the failure is due to invalid userid or password/key.

DHS-2.15.13.3 Requirement Enhancements:

The AMI component/system shall obscure feedback of authentication information during the authentication process (e.g., displaying asterisks when a user types in a password or disabling verbose error messages).

AMI components involved in authentication shall not at any time pass key or token information in an unencrypted format.

DHS-2.15.13.4 Rationale:

This control blocks several known attacks to user authentication including user enumeration, cached form field extraction, authentication sniffing, and brute force optimizations.

DHS-2.15.14 Cryptographic Module Authentication

DHS-2.15.14.1 Requirement:

The AMI component/system shall employ authentication methods that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.

DHS-2.15.14.2 Supplemental Guidance:

None.

DHS-2.15.14.3 Requirement Enhancements:

Failure of cryptographic module authentication shall not create a denial of service or adversely impact the operational performance of the AMI system. The system shall also not fail to an open unprotected state. Systems critical to overall performance, reliability, safety, and security shall provide safe secure failover protection in case of primary authentication failure.

DHS-2.15.14.4 Rationale:

Cryptographic modules are the core of the authentication process and shall be protected. These modules are frequent targets for attackers.

DHS-2.15.15 Information Flow Enforcement

DHS-2.15.15.1 Requirement:

The AMI component/system shall enforce assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy. As stated earlier, the ESI interface shall not pass control signals from the ESI to the utility, nor provide remote administration of AMI components..

DHS-2.15.15.2 Supplemental Guidance:

Information flow control regulates where information is allowed to travel within an AMI system and between AMI components (as opposed to who is allowed to access the information) without explicit regard to subsequent accesses to that information. A few general examples of possible restrictions that are better expressed as flow control than access control are: keeping export controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization and not passing any web requests to the Internet that are not from the internal web proxy. Information flow control policies and enforcement mechanisms are commonly employed by organizations to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within AMI system and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways,

guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict AMI system services or provide a packet-filtering capability.

DHS-2.15.15.3 Requirement Enhancements:

1. The information system shall implement information flow control enforcement using explicit labels on information, source, and destination objects as a basis for flow control decisions. Information flow control enforcement using explicit labels is used, for example, to control the release of certain types of information.
2. The information system shall implement information flow control enforcement using protected processing domains (e.g., domain type-enforcement) as a basis for flow control decisions.
3. The information system shall implement information flow control enforcement using dynamic security policy mechanisms as a basis for flow control decisions.

DHS-2.15.15.4 Rationale:

Restricting data flows inside a system prevents data from unintentional leakage to other parts of the AMI system. Regulation of this information flow can also decrease the attack surface of the overall AMI system from any given AMI component.

DHS-2.15.16 Passwords

DHS-2.15.16.1 Requirement:

The organization develops and enforces policies and procedures for control system users concerning the generation and use of passwords. The AMI components that support passwords shall enforce a level of complexity based on the criticality level of the device/system. Default passwords of applications, operating systems, etc shall be changed immediately. Passwords shall be changed regularly and systems should enforce an expiration policy based on the criticality level of the AMI component/system. Passwords shall not to be embedded into tools, source code, scripts, aliases or shortcuts.

DHS-2.15.16.2 Supplemental Guidance:

None.

DHS-2.15.16.3 Requirement Enhancements:

1. Default passwords of applications, operating systems, database management systems, or other programs shall be changed immediately after installation.
2. All AMI components shall allow the changing of default usernames. Passwords need to be allocated, protected, and used based on the criticality level of the systems to be accessed.

3. All AMI components that support passwords should enforce a level of complexity (min/max 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 AMI system applications, there are some cases where they are of benefit such as for local or remote access. These passwords are developed to meet defined metrics.
4. Good security practices shall 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 shall be changed immediately on first log-in. Following generation, passwords shall not be sent across any network unless protected by encryption or salted cryptographic hash specifically designed to prevent replay attacks.
5. Passwords shall be transferred to the user via secure media and the recipient shall be verified. The logon ID and password shall be never combined in the same communication.
6. The authority to keep and change high-level passwords shall be given to a trusted employee who is available during emergencies.
7. A log for master passwords needs to be maintained separately from the AMI system, possibly in a notebook in a vault or safe.
8. Passwords shall be changed regularly and expire when the user leaves the organization or after an extended period of inactivity.
9. 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 shall not to be embedded into tools, source code, scripts, aliases or shortcuts.

DHS-2.15.16.4 Rationale:

Complexity and expiration help defend against password attacks.

DHS-2.15.17 System Use Notification

DHS-2.15.17.1 Requirement:

All user interfaces to the AMI system or component shall support the ability to display an approved, system use notification message before granting access.

DHS-2.15.17.2 Supplemental Guidance:

None.

DHS-2.15.17.3 Requirement Enhancements:

The AMI system shall display an approved, system-use notification message at the time of AMI system login informing the user:

1. Of the organization's privacy policy before granting system access to potential users and/or workstations;
2. That system usage may be monitored, recorded, and subject to audit;
3. That unauthorized use of the system is prohibited and subject to criminal and civil penalties;
4. That use of the system indicates consent to monitoring and recording.

The system use notification message shall provide appropriate privacy and security notices (based on organization's associated privacy and security policies or summaries) and remain on the screen until the user takes explicit actions to log on to AMI system.

Privacy and security policies shall be consistent with applicable federal and state laws, organization directives, policies, regulations, standards, and guidance.

DHS-2.15.17.4 Rationale:

Primarily to provide legal documentation and defense for a company. This also serves as a method of user education.

DHS-2.15.18 Concurrent Session Control

DHS-2.15.18.1 Requirement:

The AMI components shall have the ability to limit the number of concurrent sessions for any user on the AMI system.

DHS-2.15.18.2 Supplemental Guidance:

The default configuration should be set to disallow concurrent logins. If a company deems it necessary to allow concurrent logins, this default can be changed. We recommend keeping the concurrent number of sessions to the smallest number possbible.

DHS-2.15.18.3 Requirement Enhancements:

None.

DHS-2.15.18.4 Rationale:

Limiting concurrent sessions enforces sounds security practices by preventing multiple users from using a single account or logging into the system from more than one machine at a time.

DHS-2.15.19 Previous Logon Notification

DHS-2.15.19.1 Requirement:

The AMI components shall notify the user, upon successful logon, of the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon based on the criticality level of the component.

DHS-2.15.19.2 Supplemental Guidance:

None.

DHS-2.12.19.3 Requirement Enhancements:

None.

DHS-2.12.19.4 Requirement Enhancements:

This allows users to aid in the detection of unauthorized use of their accounts.

DHS-2.15.20 Unsuccessful Login Attempts

DHS-2.15.20.1 Requirement:

The AMI components with user interfaces shall limit the number of consecutive invalid access attempts by a user during a given time period. The component disables user accounts when the maximum number of unsuccessful attempts is exceeded and logs all unsuccessful login attempts.

The AMI system shall limit the number of consecutive invalid access attempts by a user during a given time period. The AMI system shall temporarily disable the user account when the maximum number of unsuccessful attempts is exceeded and logs all unsuccessful login attempts.

DHS-2.15.20.2 Supplemental Guidance:

Because of the potential for denial of service, automatic lockouts initiated by the AMI system are usually temporary and automatically released after a predetermined time period established by the organization. Permanent automatic lockouts initiated by the AMI system shall be carefully considered before being used due to safety considerations and the potential for denial of service.

DHS-2.15.20.3 Requirement Enhancements:

The AMI system shall automatically lock the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

DHS-2.15.20.4 Rationale:

The limited of unsuccessful login attempts aides in deterring brute force attempts.

DHS-2.15.21 Session Lock

DHS-2.15.21.1 Requirement:

After a predetermined period of inactivity, all AMI system with user interfaces shall prevent further access to the system by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures.

DHS-2.15.21.2 Supplemental Guidance:

Users can directly initiate session lock mechanisms. A session lock is not a substitute for logging out of the AMI system. A 5-15 minute period is recommended.

DHS-2.15.21.3 Requirement Enhancements:

None.

DHS-2.15.21.4 Rationale:

This prevents users from accidentally forgetting to log out of user interfaces.

DHS-2.15.22 Remote Session Termination

DHS-2.15.22.1 Requirement:

The AMI system shall automatically terminate a remote session after a defined period of inactivity for workstations that are used for AMI system monitoring and maintenance activities based on the risk assessment of the AMI system and the organization's security policy.

On critical high-risk systems it may also be advised that the ports and/or software applications for remote access shall be disabled and in some cases physically disconnected

DHS-2.15.22.2 Supplemental Guidance:

A remote session is initiated whenever an organizational AMI system is accessed by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Some AMI components may not or cannot allow sessions to be terminated.

DHS-2.15.22.3 Requirement Enhancements:

Automatic session termination applies to local and remote sessions. The AMI system terminates a network connection at the end of a session or after a period of inactivity per organization policy and procedures.

DHS-2.15.22.3 Rationale:

This prevents users from accidentally forgetting to log out of user interfaces.

DHS-2.15.24 Remote Access

DHS-2.15.24.1 Requirement:

AMI components with remote access shall allow access to be enabled only in accordance with the appropriate policy as well as when appropriate and with a level of authentication appropriate to the criticality of the system.

DHS-2.15.24.2 Supplemental Guidance:

Remote access is any access to the AMI system or components by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Remote access includes wireless and access via portable and mobile devices. Examples of remote access methods include dial-up, broadband, and wireless. Remote access security requirements are applicable to AMI components other than public web servers or systems specifically designed for public access. The organization restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology).

Remote access to AMI component locations (e.g., control center, field locations) is only enabled when necessary, approved, and authenticated. The organization considers multifactor authentication for remote user access to the AMI system.

DHS-2.15.24.3 Requirement Enhancements:

The organization shall document, monitor, and manage all methods of remote access (e.g., dialup, Internet, physical) to the AMI system. Appropriate authentication methods are required to adequately secure remote access.

1. The organization shall employ automated mechanisms to facilitate the monitoring and control of remote access methods and all activity conducted during the remote access.
2. The organization shall use cryptography to protect the confidentiality and integrity of remote access sessions. Any latency induced from the use of cryptography, shall not degrade the operational performance of the AMI system.
3. The organization shall provide remote accesses through a limited number of managed access control points.

4. The organization shall permit remote access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan for the AMI system.

DHS-2.15.24.4 Rationale:

AMI components with remote access are primary targets for attackers because they can be exploited without physical access or risk of their physical person.

DHS-2.15.25 Access Control for Portable and Mobile Devices

DHS-2.15.25.1 Requirement:

The organization shall:

1. Establish use restrictions and implementation guidance for all portable media and mobile IT devices
2. Document, monitor, log, and limit access of these portable media and mobile devices to AMI system. Appropriate organizational officials authorize the use of portable and mobile devices per organization's established security policy and procedures.

DHS-2.15.25.2 Supplemental Guidance:

Portable media and mobile devices (e.g., notebook computers, workstations, and personal digital assistants) are allowed access to organizational networks and AMI system by meeting organizational security policies and procedures. Security policies and procedures include such activities as scanning the components for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless).

DHS-2.15.25.3 Requirement Enhancements:

Organizations shall disable unused or unnecessary I/O ports.

DHS-2.15.26 Wireless Access Restrictions

DHS-2.15.26.1 Requirement:

The AMI system shall provide the capabilities to:

1. Establish use restrictions and implementation guidance for wireless technologies
2. Authorize, monitor, and manage wireless access to the AMI system.

DHS-2.15.26.2 Supplemental Guidance:

Wireless technologies include, but are not limited to, microwave, satellite, packet radio [UHF/VHF], 802.11, 802.15, 802.16, cellular, ZigBee, ISA100, WiHart, and Bluetooth.

Scans for wireless access points should be performed in a manner that does not impact critcal system functions.

DHS-2.15.26.3 Requirement Enhancements:

The AMI system shall use authentication and cryptography or enhanced defense mechanisms to protect wireless access.

1. Any latency induced from the use of cryptography, shall not degrade the operational performance of the AMI system.
2. The organization shall scan for unauthorized wireless access points at a specified frequency and takes appropriate action if such access points are discovered. Organizations conduct a thorough scan for unauthorized wireless access points in facilities containing high-impact AMI components. The scan is not limited to only those areas within the facility containing the high-impact AMI components.

DHS-2.15.26.4 Rationale:

Wireless networks allow any attackers to obtain data passing through it. This data shall be protected from unauthorized access various attacks such as sniffing and spoofing.

DHS-2.15.27 Untrusted IT Equipment

DHS-2.15.27.1 Requirement:

The organization shall restrict the use of untrusted IT equipment as defined by the asset owner from access to the AMI system or AMI system user workstations that are used for official organization business. Untrusted equipment are those devices which have not been verified to fulfill the organization's security control requirements.This includes the processing, storage, or transmission of organization business and critical AMI system information. The terms and conditions need to address, at a minimum;

1. The types of applications that can be accessed from untrusted IT equipment, either remotely or from within the AMI system;
2. The maximum security category of information that can processed, stored, and transmitted;
3. How other users of untrusted IT equipment will be prevented from accessing organization information;
4. The use of virtual private networking (VPN) and firewall technologies;
5. The use of and protection against the vulnerabilities of wireless technologies;
6. The maintenance of adequate physical security mechanisms;
7. The use of virus and spyware protection software; and

8. How often the security capabilities of installed software are to be updated (e.g., operating system and other software security patches, virus definitions, firewall version updates, malware definitions).

DHS-2.15.27.2 Supplemental Guidance:

The organization should establish strict terms and conditions for the use of untrusted IT equipment with AMI components.

DHS-2.15.27.3 Requirement Enhancements:

None.

DHS-2.15.28 External Access Protections

DHS-2.15.28.1 Requirement:

The organization shall employ mechanisms in the design and implementation of an AMI system to restrict public access to the AMI system from the organization's enterprise network.

DHS-2.15.28.2 Supplemental Guidance:

Public access is defined as access from the enterprise system. Care should be taken to ensure data shared with the enterprise system are protected for integrity of the information and applications. Public access to the AMI system to satisfy business requirements needs to be limited to read only access through the corporate enterprise systems via a demilitarized zone (DMZ).

DHS-2.15.28.3 Requirement Enhancements:

The organization shall explicitly allow necessary network protocols in the DMZ; blocks or filters unnecessary protocols, configure firewalls to block inbound connections, limits outbound connections to only those specifically required for operations, and eliminates network connections that bypass perimeter protection mechanisms (e.g. firewall, VPN, DMZ).

DHS-2.15.29 Use of External Information Control Systems

DHS-2.15.29.1 Requirement:

The organization shall establish terms and conditions for authorized individuals to:

1. Access the AMI system from an external system;
2. Process, store, and/or transmit organization-controlled information using an external system.
3. The organization shall establish terms and conditions for the use of external information systems in accordance with organizational security policies and

procedures. The terms and conditions address, as a minimum the types of applications that can be accessed on the organizational information system from the external information system.

DHS-2.15.29.2 Supplemental Guidance:

External systems are systems or components of systems that are outside of the accreditation boundary established by the organization and for which the organization typically has no control over the application of required security levels or the assessment of security effectiveness. External information systems include, but are not limited to, personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants); privately owned computing and communications components resident in commercial or public facilities (e.g., hotels, convention centers, or airports); information systems owned or controlled by nonfederal governmental organizations; and federal information systems that are not owned by, operated by, or under the direct control of the organization.

Authorized individuals include organizational personnel, contractors, or any other individuals with authorized access to the organizational information system. This control does not apply to the use of external information systems to access organizational information systems and information that are intended for public access (e.g., individuals accessing federal information through public interfaces to organizational information systems).

DHS-2.15.29.3 Requirement Enhancements:

The organization prohibits authorized individuals from using an external system to access the AMI system or to process, store, or transmit organization-controlled information except in situations where the organization: 1) can verify the employment of required security mechanisms on the external system as specified in the organization's security policy and system security plan; or 2) has approved system connection or processing agreements with the organizational entity hosting the external system.

AMISP-2.15.2 Unauthorized Access Reporting

AMISP-2.15.2.1 Requirement:

The AMI components shall record and report the following security events.

1. Unauthorized and unsuccessful attempts to access the system

AMISP-2.15.2.2 Supplemental Guidance

This can be accomplished with a number of approaches including:

1. System Use Notification (DHS-2.15.17, DHS-2.15.19, DHS-2.15.20)
2. Previous Logon Notification
3. Unsuccessful Login Attempts

AMISP-2.15.2.3 Requirement Enhancements:

None.

AMISP-2.15.2.4 Rationale:

This data is necessary to audit and detect attack attempts.

2.16 Audit and Accountability

Periodic audits and logging of the AMI components and 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 are also used to detect breaches in security services through examination of system logs. Logging is necessary for anomaly detection as well as forensic analysis.

DHS-2.16.2 Auditable Events

DHS-2.16.2.1 Requirement:

All AMI components shall generate audit records, at a minimum, for the following events whether or not the attempts were successful:

1. Security Events
2. Control Events
3. System/Device Configuration Changes

All AMI systems and components shall transmit all audit records and logs to a dedicated log management system. Audit record generation and processing shall not degrade the operational performance of the AMI components or system.

DHS-2.16.2.2 Supplemental Guidance:

Auditing activity can affect AMI system performance; therefore, the organization decides, based on a risk assessment, which events require auditing continually and which events require auditing in response to specific situations.

The purpose of this requirement is to identify significant and relevant events to the security of the AMI system that needs to be audited. The organization specifies which AMI components carry out auditing activities. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems.

DHS-2.16.2.3 Requirement Enhancements:

The organization shall specify which AMI system components carry out auditing activities and ensure that certain events are included or excluded from the set of auditable events based on specified attributes.

The organization defines auditable events that are adequate to support after-the-fact investigations of security incidents.

The targeted security functionality shall be able to generate an audit record of:

1. Startup and shutdown of the audit functions;
2. Successful and failed logins
3. Failed authentications of signed or encrypted requests
4. Change in access control or privilege
5. Changes to security settings
6. Creation, deletion, or modifications of users, password, tokens, and security keys
7. Triggering of tamper sensors

The organization shall maintain a centralized log management system for long term storage and log correlation. This system shall:

1. Provide the capability to compile audit records from multiple components throughout the system into a system wide (logical or physical), time-correlated audit trail.
2. Provide the capability to manage the selection of events to be audited by individual components of the system.
3. Provide the organization the ability to periodically review and update the list of organization-defined auditable events.

DHS-2.16.2.4 Rationale

A utility's ability to monitor and audit activity on the AMI system will be limited by the functionality provided by the individual system components. Traditionally, process control system components provided little or no support for logging capabilities and relied on perimeter control components to detect anomalous or malicious activity. The geographically diverse architecture of an AMI system is not compatible with this strategy and therefore, all AMI system components should provide the ability to generate security and event logs to adequately address this need.

DHS-2.16.3 Content of Audit Records

DHS-2.16.3.1 Requirement:

All AMI components shall capture sufficient and detailed information in audit records to establish what events occurred, the sources of the events, and their outcomes.

DHS-2.16.3.2 Supplemental Guidance:

Two types of audits should be tracked:

1. General quality assurance audits of the configuration and operation of the AMI system that verify compliance with organization's security plan;
2. Audits of operational events encountered by the AMI system when the system operates outsides its normal operating parameters.

General quality assurance audit records contain information of what was audited and the results of the audit; that is, the system is in compliance or not, and if not, what areas are out of compliance. Operational event audits are initiated by the organization's corrective action process when the AMI system operates outsides its normal operating parameters.

Audit record content typically includes:

1. Date and time of the event;
2. The component of the AMI system (e.g., software or hardware component) where the event occurred;
3. Type of event;
4. User/subject/device identity;
5. The operational consequences in the case of an operational event.

DHS-2.16.3.3 Requirement Enhancements:

Two types of audits shall be tracked:

3. General quality assurance audits of the configuration and operation of the AMI system that verify compliance with organization's security plan;
4. Audits of operational events encountered by the AMI system when the system operates outsides its normal operating parameters.

All AMI components shall provide the capability to include additional, more detailed information in the records for audit events identified by type, location, or subject. All AMI systems and components shall provide the capability to centrally manage the content of audit records generated by individual components throughout the AMI system.

DHS-2.16.3.4 Rationale:

The content of the security logs generated by the various AMI system components is driven by the need to detect various situations within the system. Log contents shall provide sufficient information so that scenarios such as abnormal operation of the AMI system, attacks on the AMI system or component, and inappropriate use of the AMI system can be detected.

DHS-2.16.4 Audit Storage Capacity

DHS-2.16.4.1 Requirement:

All AMI components shall provide sufficient audit record storage capacity and capabilities to configure auditing to reduce the likelihood of such capacity being exceeded.

Under normal usage conditions, components and systems shall store events locally for the following minimal timeframes:

1. Embedded Devices: 1 week
2. Traditional IT or SCADA Servers: 1 month
3. Central Log Management Systems: 1 year

Under anomalous usage conditions, components and system shall store events locally for the following minimal timeframes:

1. Embedded Devices:
2. Traditional IT or SCADA Server:
3. Central Log Management Systems:

DHS-2.16.4.2 Supplemental Guidance:

None.

DHS-2.16.4.3 Requirement Enhancements:

None.

DHS-2.16.4.4 Rationale:

Log storage is critical in a utility's compliance reporting and auditing efforts and therefore the most critical requirements for log storage are focused on the Central Log Management System which is the primary tool utilized for this purpose. Requirements applicable to end devices which generate the security logs are focused on the devices ability to deliver the logs to the Central Log Management System under various failure and attack scenarios. Logs should be kept in accordance NERC CIP requirements.

DHS-2.16.5 Response to Audit Processing Failures

DHS-2.16.5.1 Requirement:

The log management system shall alert appropriate organization personnel in case of audit failure events, such as:

1. Allocated audit record storage volume reaches organization-defined percentage of maximum audit record storage capacity.
2. Log management systems have not received log messages from a particular AMI component for a configurable period of time.
3. Inability to read from or write to the event storage volume.

Actions for handling log management system alerts shall be defined and determined by the utility

DHS-2.16.5.2 Supplemental Guidance:

Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

DHS-2.16.5.3 Requirement Enhancements:

1. The AMI system provides a warning when allocated audit record storage volume reaches organization-defined percentage of maximum audit record storage capacity;
2. The AMI system provides a real-time alert when the following organization defined audit failure events occur.

DHS-2.16.5.4 Rationale:

Without access to security logs, asset owners are vulnerable to security events within the AMI system going undetected. Ensuring that all AMI system components utilized to generate, store, and analyze these logs are operating as intended is of the utmost importance and anomalies or failures should be alerted and dealt with as a high priority issue.

DHS-2.16.7 Audit Reduction and Report Generation

DHS-2.16.7.1 Requirement:

The dedicated log management systems shall provide an audit reduction and report generation capability.

DHS-2.16.7.2 Supplemental Guidance:

Audit reduction, review, and reporting tools support after-the-fact investigations of security incidents without altering original audit records.

DHS-2.16.7.3 Requirement Enhancements:

None.

DHS-2.16.7.4 Rationale:

Asset owners operating AMI systems need to collect, store and analyze huge amounts of security event data from the various components within the system. As no standards exist on the content and syntax of these logs, variations exist between components provided by different manufacturers and analysis of the raw logs is often time consuming or impractical. Without tools capable of filtering, parsing, normalizing, and correlating this data, the utilities ability to quickly respond to potential security events may be limited. It is important to note however, this requirement cannot supersede the requirements to protect these logs identified in DHS-2.16.9.

DHS-2.16.8 Time Stamps

DHS-2.16.8.1 Requirement:

All AMI system and components shall provide time stamps for use in audit record generation.

DHS-2.16.8.2 Supplemental Guidance:

Redundant, verifiable time sources should be used.

DHS-2.16.8.3 Requirement Enhancements:

Time stamps of audit records shall be generated using internal system clocks synchronized across all of the AMI components.

DHS-2.16.8.4 Rationale:

Log data can be reviewed chronologically to determine what was happening both before and during an event within the AMI system. For this to happen, the accuracy and coordination of clocks of the various components is critical so that timestamps within the audit records can be correlated across the AMI system. To accurately trace activity, clocks need to be regularly synchronized to a central source to ensure that the date/time stamps are in synch.

DHS-2.16.9 Protection of Audit Information

DHS-2.16.9.1 Requirement:

All AMI components and system shall protect audit information and audit tools from unauthorized access, modification, and deletion.

DHS-2.16.9.2 Supplemental Guidance:

Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit AMI system activity. The logs are important for error correction, security breach recovery, investigations, and related efforts.

DHS-2.16.9.3 Requirement Enhancements:

None.

DHS-2.16.9.4 Rationale:

For log data to be useful, it shall be secured from unauthorized access and integrity problems. The risk, real or perceived, of improperly secured logs is that an activity can occur on the AMI system for malicious purposes and then the logs altered to not show what happened. Specifically, there are many "rootkits" are specifically designed to alter the security logs to remove evidence of their installation and execution. In general, access to the logs shall be restricted to ensure their integrity which necessitates access controls as well as the use of hardened systems.

DHS-2.16.12 Auditor Qualification

DHS-2.16.12.1 Requirement:

The organization's audit program shall specify auditor qualifications in accordance with the organization's documented training program.

DHS-2.16.12.2 Supplemental Guidance:

The selection of auditors and conduct of audits should ensure the objectivity and impartiality of the audit process. Security auditors need to:

1. Understand the AMI system to be audited and be personally familiar with the systems and operating practices;
2. Understand the risk involved with the audit and the consequences associated with unintentional stimulus or denial of service to the AMI system;
3. Fully understand the corporate cyber and AMI system security policies and procedures and the specific health, safety, and environmental risks associated with a particular facility and/or process.

DHS-2.16.12.3 Requirement Enhancements:

The organization assigns auditor and system administration functions to separate personnel.

DHS-2.16.12.4 Rationale:

Although some characteristics are similar, AMI systems also have characteristics that differ from traditional information systems. These range from performance and reliability

requirements to the use operating systems and applications that may be considered unconventional to typical IT personnel. Furthermore, the goals of safety and efficiency sometimes conflict with security in the design and operation of AMI systems. For these reasons, auditors shall be familiar with the AMI system and technology utilized within it as well as the basics of power system operations.

AMISP-2.16.1 Audit Tools

AMISP-2.16.1.1 Requirement:

The organization under the audit program shall specify strict rules and careful use of audit tools when auditing AMI system functions.

AMISP-2.16.1.2 Supplemental Guidance:

As a general practice, system audits determine compliance of the AMI system to the organization's security plan. Auditing and log management tools need to be used cautiously in maintaining and proving the integrity of the AMI system from installation through the system life cycle. Access to AMI system audit tools need to be protected to prevent any possible misuse or compromise.

AMISP-2.16.1.3 Requirement Enhancements:

For new AMI components, system auditing utilities need to be incorporated into the design. Appropriate security audit practices for legacy systems require appropriate precautions be taken before assessing the AMI system. For AMI system audits to determine inappropriate activity, information custodians ensure that AMI system monitoring tools are installed to log system activity and security events.

The AMI system and its components shall continue to operate during and after a cyber security scan.

AMISP-2.16.1.3 Rationale:

Although some characteristics are similar, AMI systems also have characteristics that differ from traditional information systems. Many of these differences stem from the fact that AMI systems are integrated into the physical power grid. In some cases, adversely impacting an AMI system can pose significant risk to the health and safety of human lives and serious damage to the environment, as well as serious financial issues such as production losses. Furthermore, the goals of safety and efficiency sometimes conflict with security in the design and operation of AMI systems. For these reasons, any auditing and testing of the AMI system shall be strictly controlled.

2.17 Survivability

Survivability is the capability of a system to fulfill its mission in a timely manner despite attack, accident, or component failure. The characteristics of a survivable system include its ability to prevent or resist attacks, accidents, or other forms of stress, recognize a

survivability event and the state of the system under stress, and to recover from the adverse impact of a survivability event in a timely manner. Survivability is marked by graceful degradation under stress, with essential services maintained.

AMISP-2.17.1 Delay of Remote Connect/Disconnect

AMISP-2.17.1 Requirement:

The physical design of any device providing a remote connect/disconnect capability (whether "under the glass" of a smart meter or as a separate device) shall contribute to the prevention of adverse electrical system impacts that could be caused by a large number of simultaneous connects and/or disconnects.

AMISP-2.17.1.2 Supplemental Guidance:

The recommended physical survivability control is for the device to introduce a random delay before responding to any remote connect or disconnect command. The delay should be selected at random such that: 1) the delay to be imposed is known only at the time of the request, 2) the delay is selected uniformly in the range of 0 to 360 minutes (or greater[13]), and 3) the selection and imposition of the delay are implemented by a device whose operation, excepting disconnect/connect requests and request cancellations, cannot be modified via a network interface. Moreover, the meter should respond immediately to a *cancel remote connect/disconnect* command by cancelling any connect/disconnect command that has been received but not yet executed.[14]

AMISP-2.17.1.3 Requirement Enhancements:

The software associated with scheduling remote connects/disconnects shall recognize when a dangerously large number of remote connects/disconnects have been scheduled to occur simultaneously, provide notification of the pending anomalous event, and suspend issuing any connect/disconnect commands until the situation is understood and resolved by properly authorized utility personnel.

The remote connect/disconnect device and/or its associated infrastructure shall log sufficient information about remote connect/disconnect commands received by the device to enable subsequent troubleshooting, tracking, and other forensic analysis in the event of a suspected attack or other anomaly.

---

[13] Of course, the upper value of the range must not be so large that it obviates the usefulness of the remote connect/disconnect capability.

[14] We are assuming that the scheduling of remote connects and disconnects is done external to the meter, and that the meter receives only the command, and not a date/time at which to execute the command. The requirement that a device respond instantly to a *cancel remote connect/disconnect* command allows the utility to abort a large number of connect/disconnect commands that have been accidentally or maliciously issued, but not yet carried out.

AMISP-2-17.1.4 Rationale

The connect/disconnect capability of a smart meter makes it possible for large numbers of connects and/or disconnects to occur simultaneously through accident or malice. The resulting large and rapid fluctuations in load can cause large frequency excursions, thereby forcing generators offline, damaging electrical equipment, or both. Due to the possible severity of such impacts, physical survivability controls are needed that will be effective even if all other cyber security controls fail. The recommended control forces load changes to occur over (at least) a six hour period. This eliminates sudden, dangerous fluctuations in load and provides sufficient time for a utility to recognize and respond to an unfolding event.

Appendix A Mapping of Controls to Components

The following table maps the security controls found throughout Section 5 to the logical components found in Section 4. Each row corresponds to a subsection of Section 5. An 'x' is found in a column along each role if that control applies to component found in that column. Many controls apply to all AMI components, and are noted as such by an 'x' in the corresponding column. An 'x' may appear in multiple columns, for example when a control applies to all components but has additional guidance for a specific component, two columns (one for all and one for the specific component) will be marked.

A.1 Controls and Components Matrix

Applies to all components	Organizational	AMI Comm. Network Device	AMI Forecasting System	AMI Head End	AMI Meter	AMI Meter Management System	AMI Network Management System	DRAACS	Field Tool/Device	Grid Control Center	MDMS	Non-electric Meter	Third-party Meter/Submeter	Other exception	Comment
x															

Applies to all components	Organizational	AMI Comm. Network Device	AMI Forecasting System	AMI Head End	AMI Meter	AMI Meter Management System	AMI Network Management System	DRAACS	Field Tool/Device	Grid Control Center	MDMS	Non-electric Meter	Third-party Meter/Submeter	Other exception	Comment

Applies to all components	Organizational	AMI Comm. Network Device	AMI Forecasting System	AMI Head End	AMI Meter	AMI Meter Management System	AMI Network Management System	DRAACS	Field Tool/Device	Grid Control Center	MDMS	Non-electric Meter	Third-party Meter/Submeter	Other exception	Comment

Applies to all components	Organizational	AMI Comm. Network Device	AMI Forecasting System	AMI Head End	AMI Meter	AMI Meter Management System	AMI Network Management System	DRAACS	Field Tool/Device	Grid Control Center	MDMS	Non-electric Meter	Third-party Meter/Submeter	Other exception	Comment

Applies to all components	Organizational	AMI Comm. Network Device	AMI Forecasting System	AMI Head End	AMI Meter	AMI Meter Management System	AMI Network Management System	DRAACS	Field Tool/Device	Grid Control Center	MDMS	Non-electric Meter	Third-party Meter/Submeter	Other exception	Comment

		Applies to all components	Organizational	AMI Comm. Network Device	AMI Forecasting System	AMI Head End	AMI Meter	AMI Meter Management System	AMI Network Management System	DRAACS	Field Tool/Device	Grid Control Center	MDMS	Non-electric Meter	Third-party Meter/Submeter	Other exception	Comment
2.8 System and Communication Protection	2.8.1 System and Communication Protection Policy and Procedures		x														
	2.8.2 Management Port Partitioning	x															

	Applies to all components	Organizational	AMI Comm. Network Device	AMI Forecasting System	AMI Head End	AMI Meter	AMI Meter Management System	AMI Network Management System	DRAACS	Field Tool/Device	Grid Control Center	MDMS	Non-electric Meter	Third-party Meter/Submeter	Other exception	Comment
2.8.3 Security Function Isolation	x															
2.8.4 Information Remnants	x															
2.8.5 Denial-of-Service Protection	x														x	wireless assets
2.8.6 Resource Priority	x															
2.8.7 Boundary Protection	x															
2.8.8 Communication Integrity	x															
2.8.9 Communication Confidentiality	x															
2.8.10 Trusted Path	x															
2.8.11 Cryptographic Key Establishment and Management															x	applies to overall system
2.8.12 Use of Validated Cryptography	x															
2.8.13 Collaborative Computing	x															
2.8.14 Transmission of Security Parameters	x															
2.8.15 Public Key Infrastructure Certificates															x	applies to overall system

		Applies to all components	Organizational	AMI Comm. Network Device	AMI Forecasting System	AMI Head End	AMI Meter	AMI Meter Management System	AMI Network Management System	DRAACS	Field Tool/Device	Grid Control Center	MDMS	Non-electric Meter	Third-party Meter/Submeter	Other exception	Comment
	2.8.16 Mobile Code	x															
	2.8.17 Voice-Over Internet Protocol	x															
	2.8.18 System Connections	x															
	2.8.19 Security Roles	x															
	2.8.20 Message Authenticity	x															
	2.8.21 Architecture and Provisioning for Name/Address Resolution Service															x	applies to overall system
	2.8.22 Secure Name / Address Resolution Service (Authoritative Source)															x	
	2.8.23 Secure Name/Address Resolution Service (Recursive or Caching Resolver)															x	
2.9 Information and Document Management	2.9.1 Information and Document Management Policy and Procedures		x														

		Applies to all components	Organizational	AMI Comm. Network Device	AMI Forecasting System	AMI Head End	AMI Meter	AMI Meter Management System	AMI Network Management System	DRAACS	Field Tool/Device	Grid Control Center	MDMS	Non-electric Meter	Third-party Meter/Submeter	Other exception	Comment
	2.9.2 Information and Document Retention		x														
	2.9.3 Information Handling		x														
	2.9.4 Information Classification		x														
	2.9.5 Information Exchange		x														
	2.9.6 Information and Document Classification		x														
	2.9.7 Information and Document Retrieval		x														
	2.9.8 Information and Document Destruction		x														
	2.9.9 Information and Document Management Review		x														
	2.9.10 Automated Marking	x															
	2.9.11 Automated Labeling										x						
2.10 System Development and Maintenance	2.10.1 System Maintenance Policy and Procedures		x														

		Applies to all components	Organizational	AMI Comm. Network Device	AMI Forecasting System	AMI Head End	AMI Meter	AMI Meter Management System	AMI Network Management System	DRAACS	Field Tool/Device	Grid Control Center	MDMS	Non-electric Meter	Third-party Meter/Submeter	Other exception	Comment
	2.10.2 Legacy System Upgrades		x														
	2.10.3 System Monitoring and Evaluation		x														
	2.10.4 Backup and Recovery		x														
	2.10.5 Unplanned System Maintenance		x														
	2.10.6 Periodic System Maintenance		x														
	2.10.7 Maintenance Tools		x														
	2.10.8 Maintenance Personnel		x														
	2.10.9 Remote Maintenance		x														
	2.10.10 Timely Maintenance		x														
2.11 Security Awareness and Training	2.11.1 Security Awareness and Training Policy and Procedures																
	2.11.2 Security Awareness																

		Applies to all components	Organizational	AMI Comm. Network Device	AMI Forecasting System	AMI Head End	AMI Meter	AMI Meter Management System	AMI Network Management System	DRAACS	Field Tool/Device	Grid Control Center	MDMS	Non-electric Meter	Third-party Meter/Submeter	Other exception	Comment
	2.11.3 Security Training																
	2.11.4 Security Training Records																
	2.11.5 Contact with Security Groups and Associations																
	2.11.6 Security Responsibility Testing																
2.12 Incident Response	2.12.1 Incident Response Policy and Procedures		x														
	2.12.2 Continuity of Operations Plan		x														
	2.12.3 Continuity of Operations Roles and Responsibilities		x														
	2.12.4 Incident Response Training		x														
	2.12.5 Continuity of Operations Plan Testing		x														
	2.12.6 Continuity of Operations Plan Update		x														
	2.12.7 Incident Handling	x															

	Applies to all components	Organizational	AMI Comm. Network Device	AMI Forecasting System	AMI Head End	AMI Meter	AMI Meter Management System	AMI Network Management System	DRAACS	Field Tool/Device	Grid Control Center	MDMS	Non-electric Meter	Third-party Meter/Submeter	Other exception	Comment
2.12.8 Incident Monitoring		x														
2.12.9 Incident Reporting		x														
2.12.10 Incident Response Assistance		x														
2.12.11 Incident Response Investigation and Analysis		x														
2.12.12 Corrective Action		x														
2.12.13 Alternate Storage Sites		x														
2.12.14 Alternate Command/Control Methods						x				x						
2.12.15 Alternate Control Center		x									x					
2.12.16 Control System Backup	x	x														
2.12.17 Control System Recovery and Reconstitution	x															
2.12.18 Fail-Safe Response	x															

		Applies to all components	Organizational	AMI Comm. Network Device	AMI Forecasting System	AMI Head End	AMI Meter	AMI Meter Management System	AMI Network Management System	DRAACS	Field Tool/Device	Grid Control Center	MDMS	Non-electric Meter	Third-party Meter/Submeter	Other exception	Comment
2.13 Media Protection	2.13.1 Media Protection Policy and Procedures																
	2.13.2 Media Access																
	2.13.3 Media Classification																
	2.13.4 Media Labeling																
	2.13.5 Media Storage																
	2.13.6 Media Transport																
	2.13.7 Media Sanitization and Disposal																
2.14 System and Information Integrity	2.14.1 System and Information Integrity Policy and Procedures		x														
	2.14.2 Flaw Remediation		x														
	2.14.3 Malicious Code Protection	x															
	2.14.4 System Monitoring Tools and Techniques	x															
	2.14.5 Security Alerts and Advisories		x														

		Applies to all components	Organizational	AMI Comm. Network Device	AMI Forecasting System	AMI Head End	AMI Meter	AMI Meter Management System	AMI Network Management System	DRAACS	Field Tool/Device	Grid Control Center	MDMS	Non-electric Meter	Third-party Meter/Submeter	Other exception	Comment
	2.14.6 Security Functionality Verification	x															
	2.14.7 Software and Information Integrity	x															
	2.14.8 Spam Protection	x															
	2.14.9 Information Input Restrictions	x															
	2.14.10 Information Input Accuracy, Completeness, Validity, and Authenticity	x															
	2.14.11 Error Handling	x															
	2.14.12 Information Output Handling and Retention		x														
2.15 Access Control	2.15.1 Access Control Policy and Procedures	x					x										
	2.15.2 Identification and Authentication Policy and Procedures	x	x				x										
	2.15.3 Account Management	x	x														
	2.15.4 Identifier Management	x	x														

	Applies to all components	Organizational	AMI Comm. Network Device	AMI Forecasting System	AMI Head End	AMI Meter	AMI Meter Management System	AMI Network Management System	DRAACS	Field Tool/Device	Grid Control Center	MDMS	Non-electric Meter	Third-party Meter/Submeter	Other exception	Comment
2.15.5 Authenticator Management	x	x														
2.15.6 Supervision and Review		x														
2.15.7 Access Enforcement	x															
2.15.8 Separation of Duties	x															
2.15.9 Least Privilege	x															
2.15.10 User Identification and Authentication	x															
2.15.11 Permitted Actions Without Identification or Authentication	x															
2.15.12 Device Identification and Authentication	x															
2.15.13 Authenticator Feedback	x															
2.15.14 Cryptographic Module Authentication	x															
2.15.15 Information Flow Enforcement	x															
2.15.16 Passwords	x															

	Applies to all components	Organizational	AMI Comm. Network Device	AMI Forecasting System	AMI Head End	AMI Meter	AMI Meter Management System	AMI Network Management System	DRAACS	Field Tool/Device	Grid Control Center	MDMS	Non-electric Meter	Third-party Meter/Submeter	Other exception	Comment
2.15.17 System Use Notification	x															
2.15.18 Concurrent Session Control	x															
2.15.19 Previous Logon Notification	x															
2.15.20 Unsuccessful Login Attempts	x															
2.15.21 Session Lock	x															
2.15.22 Remote Session Termination	x															
2.15.23 Remote Access Policy and Procedures		x														
2.15.24 Remote Access	x															
2.15.25 Access Control for Portable and Mobile Devices		x														
2.15.26 Wireless Access Restrictions																
2.15.27 Personally Owned Information		x														
2.15.28 External Access Protections		x														

		Applies to all components	Organizational	AMI Comm. Network Device	AMI Forecasting System	AMI Head End	AMI Meter	AMI Meter Management System	AMI Network Management System	DRAACS	Field Tool/Device	Grid Control Center	MDMS	Non-electric Meter	Third-party Meter/Submeter	Other exception	Comment
	2.15.29 Use of External Information Control Systems	x															
2.16 Audit and Accountability	2.16.1 Audit and Accountability Policy and Procedures		X														
	2.16.2 Auditable Events	X															
	2.16.3 Content of Audit Records	X															
	2.16.4 Audit Storage Capacity	X															
	2.16.5 Response to Audit Processing Failures															X	Log Management System
	2.16.6 Audit Monitoring, Analysis, and Reporting		X														
	2.16.7 Audit Reduction and Report Generation															X	Log Management System
	2.16.8 Time Stamps	X															
	2.16.9 Protection of Audit Information	X															

	Applies to all components	Organizational	AMI Comm. Network Device	AMI Forecasting System	AMI Head End	AMI Meter	AMI Meter Management System	AMI Network Management System	DRAACS	Field Tool/Device	Grid Control Center	MDMS	Non-electric Meter	Third-party Meter/Submeter	Other exception	Comment
2.16.10 Audit Record Retention		X														
2.16.11 Conduct and Frequency of Audits		X														
2.16.12 Auditor Qualification	X															
2.16.13 Audit Tools															X	Audit Tools
2.16.14 Security Policy Compliance		X														

Appendix B Communication throughout the AMI Logical Architecture

The following table identifies the detailed communications (information exchange and control signals) between components and actors found in the AMI Logical Architecture defined in Section 4.2

Each row corresponds to communications between two components/actors in a given direction (the component in parenthesis is the recipient of the communication). The second column notes all separate communications for this row, as derived from the AMI Enterprise use cases documented on SmartGridiPedia (http://www.smartgridipedia.org/index.php/Use_Cases_with_Integration_Requirements).

Each communication is mapped to the corresponding source scenario in the third column. The convention used in this column is use case number – scenario number(s); e.g., B1 – Sc1 denotes use case B1, scenario 1. This information is included for traceability.

Information in Transit		
Link (Destination)	Information	Reference
1 (Head End)	Meter reading	B1 – Sc1, Sc2; B2 – Sc1, Sc2, Sc3; D3 – Sc1
	Meter event	B1 – Sc3
	"Read" schedule ack	B1 – Sc6
	Successful turn off confirmation	B2 – Sc1, Sc3
	Meter energized status	B2 – Sc2
	Successful turn on confirmation	B2 – Sc2
	Load limit confirmation	B2 – Sc6
	Removal event	B3 – Sc1
	Re-installation event	B3 – Sc1
	Inversion event	B3 – Sc3
	Customer load detected event	B3 – Sc4
	Physical intrusion event	B3 – Sc5
	Meter tampering attempt, outage, or restoration event	B3 – Sc6; I2 – Sc7
	Event (load shed) notification confirmation	CDR&LC
	Event (load shed) start confirmation	CDR&LC

Information in Transit		
Link (Destination)	Information	Reference
	Event (load shed) end confirmation	CDR&LC
	Meter provisioning request confirmation	C2 – Sc2
	HAN communication confirmation	C2 – Sc2
	Informational message receipt conformation	C2 – Sc5
	Prepay meter event (i.e. credit mode)	C3 – Sc4
	Customer HAN equipment response	C4 – Sc1
	Power Quality event	D2 – Sc1
	Power Quality data response	D2 – Sc1
	Real-time data response (volts, watts, PF, etc.)	D2 – Sc3
	Successful meter program confirmation	D3 – Sc1
	Unexpected/unauthorized DG notification	D3 – Sc2, Sc3
	Self-registration	I1 – Sc1, Sc2
	Error event or self-test failure	I2 – Sc8
	Event log	I3 – Sc1
	Restoration event (and status)	S1 – Sc1, Sc2
1 (Meter)	On-demand meter read request	B1 – Sc2
	"Read" schedule	B1 – Sc6

Information in Transit		
Link (Destination)	Information	Reference
	Scheduled turn off notification	B2 – Sc1
	Scheduled turn off command	B2 – Sc1
	Request meter energized status	B2 – Sc2
	Scheduled turn on command	B2 – Sc2
	On demand turn off command	B2 – Sc3
	Load limit command	B2 – Sc6
	Removal event confirmation	B3 – Sc1
	Re-installation event confirmation	B3 – Sc1
	Load shed command	CDR&LC
	Electric Price Data	C2 – Sc1
	Meter Provisioning Request (New HAN Display Device)	C2 – Sc2
	Informational message	C2 – Sc5
	Prepayment service message	C3 – Sc1, Sc4
	Prepayment status message	C3 – Sc2
	Customer HAN equipment command	C4 – Sc1
	Power Quality data request	D2 – Sc1
	Real-time data request (volts, watts, PF, etc.)	D2 – Sc3

Information in Transit		
Link (Destination)	Information	Reference
	Meter programming (i.e. tariff)	D3 – Sc1
	Planned outage information	D4 – Sc3
	Reconfigure meter asset	I1 – Sc1
	Execute firmware command	I3 – Sc1
	Updated firmware	I3 – Sc1
2 (MDMS)	Meter reading	B1 – Sc1, Sc2, Sc8; B2 – Sc1, Sc2, Sc3; B4 – Sc1; D3 – Sc1
	Meter event	B1 - Sc3; B4 – Sc5, Sc6
	Failed on-demand read	B1 – Sc16
	Load shed control confirmation	CDR&LC
	Load shed control start confirmation	CDR&LC
	Load shed control end confirmation	CDR&LC
	Demand Response Confirmation Failure	C1 – Sc2
	Prepay meter event (i.e. credit mode)	C3 – Sc4
	Customer HAN equipment response	C4 – Sc1
	Successful meter program confirmation	D3 – Sc1
	Unexpected/unauthorized DG notification	D3 – Sc2, Sc3

Information in Transit		
Link (Destination)	Information	Reference
	Power outage notification	D4 – Sc1
	Power restoration notification	D4 – Sc1
	Event log	I3 – Sc1
2 (Head End)	On-demand meter read request	B1 – Sc2, Sc8; S1 – Sc3
	Request non-electric meter event monitoring	B4 – Sc5
	Load shed command	CDR&LC
	Prepayment service message	C3 – Sc4
	Customer HAN equipment command	C4 – Sc1
	Meter programming (i.e. tariff)	D3 – Sc1
	Planned outage information	D4 – Sc3
3 (MDMS)	On-demand meter read request	B1 – Sc2
	Meter event ack	B1 – Sc3
	Data request	B1 – Sc5
	Meter data anomaly	I2 – Sc6
3 (Data Retriever)	Meter reading	B1 – Sc2
	Meter event	B1 – Sc3

Information in Transit		
Link (Destination)	Information	Reference
	Requested data Failed on-demand read Results of service order	B1 – Sc5 B1 – Sc16 I2 – Sc6
4 (MDMS)	Request meter read data Request non-electric meter event monitoring Customer energy data request Customer HAN equipment command	B1 – Sc7, Sc8; B4 – Sc1 B4 – Sc5 C2 – Sc3 C4 – Sc1
4 (Data Portal)	Meter reading Non-electric meter event Customer energy data Customer HAN equipment response	B1 – Sc7, Sc8; B4 – Sc1 B4 – Sc5, Sc6 C2 – Sc3 C4 – Sc1
5 (Data Portal)	*Meter data request* *Customer HAN equipment command*	*B1 – Sc7* *C4 – Sc1*
5 (Third Party Org)	*Meter reading* *Customer HAN equipment response*	*B1 – Sc7* *C4 – Sc1*
6 (Third Party Meter)	On-demand meter read request	B1 – Sc8

Information in Transit		
Link (Destination)	Information	Reference
6 (Head End)	Meter reading	B1 – Sc8
7 (Head End Operator)	Meter reading report (re: unresponsive meters)	B1 – Sc9
7 (Head End)		
8 (Field Person)	Pickup read request	B1 – Sc12
8 (MDMS)		
9 (Meter)	Request all meter data (and logs) Credentials for Field Person's communication Command to turn on/off electric service Meter configuration data Request self-test results and communication test	B1 – Sc12; I2 – Sc1 B2 – Sc2 B2 – Sc2 I2 – Sc1 I2 – Sc1
9 (Field Tool)	All stored meter data (and logs) Acceptance of credentials Confirmation of turn on/off electric service Meter reading Meter ID	B1 – Sc12; I2 – Sc1 B2 – Sc2 B2 – Sc2 B2 – Sc2 I1 – Sc1

Information in Transit		
Link (Destination)	Information	Reference
	Success of AMI system registration Meter test results	I1 – Sc1 I2 – Sc1
10 (MDMS)	All stored meter data	B1 – Sc12
10 (Field Tool)		
11 (AMI Meter Mgmt System)	Problem meters report Meter service order request Meter reading	B1 – Sc15 I2 – Sc6 I3 – Sc1
11 (MDMS)	Closed meter order status Meter reading request	I2 – Sc6 I3 – Sc1
12 (Head End Operator)	Meter service order	B1 – Sc15
12 (AMI Meter Mgmt System)	Schedule upgrade	I3 – Sc1
13 (MDMS)	Request billing determinant Prepayment request DG enrollment information	B1 – Sc17 C3 – Sc4 D3 – Sc1

Information in Transit		
Link (Destination)	Information	Reference
13 (CIS)	Billing determinant	B1 – Sc17
	Prepay meter event (i.e. credit mode)	C3 – Sc4
	Successful meter program confirmation	D3 – Sc1
	Unexpected/unauthorized DG notification	D3 – Sc2, Sc3
14 (CIS)	*Disconnect request*	*B2 – Sc1*
	Request to establish service	*B2 – Sc2*
	HAN Display Device provisioning request	*C2 – Sc2*
	Prepayment request	*C3 – Sc1*
	Prepayment information	*C3 – Sc1*
	DG enrollment request	*D3 – Sc1*
	Request meter service	*I2 – Sc3*
	HAN device asset ID	*I3 – Sc2, Sc3*
14 (Customer)	*HAN Display Device test message receipt confirmation*	*C2 – Sc2*
	Prepayment balance approaching zero message	*C3 – Sc3*
	DG ready for use notification	*D3 – Sc1*
	Unexpected/unauthorized DG notification	*D3 – Sc2, Sc3*

Information in Transit		
Link (Destination)	Information	Reference
15 (Head End)	Scheduled turn off notification	B2 – Sc1
	Scheduled turn off command	B2 – Sc1
	Request meter energized status	B2 – Sc2
	Scheduled turn on command	B2 – Sc2
	On demand turn off command	B2 – Sc3
	Load limit command	B2 – Sc6
	Electric Price Data	C2 – Sc1
	Meter Provisioning Request (New HAN Display Device)	C2 – Sc2
	Informational message	C2 – Sc5
	Prepayment service message	C3 – Sc1
	Rate change message	C3 – Sc1
15 (CIS)	Successful turn off confirmation	B2 – Sc1, Sc3
	Energized meter status	B2 – Sc2
	Successful turn on confirmation	B2 – Sc2
	Load limit confirmation	B2 – Sc6
	Meter provisioning request confirmation	C2 – Sc2
	HAN communication confirmation	C2 – Sc2

Information in Transit		
Link (Destination)	Information	Reference
	Informational message receipt conformation	C2 – Sc5
16 (HAN Display)	Scheduled turn off notification	B2 – Sc1
	Load limit notification and usage data	B2 – Sc6
	Load control event notification	CDR&LC
	Event start message	CDR&LC
	Event end message	CDR&LC
	Electric Price Data	C2 – Sc1
	Energy Consumption Data	C2 – Sc1
	Test message	C2 – Sc2
	Informational message	C2 – Sc5
	Prepayment status	C3 – Sc1, Sc2, Sc4
	Prepay meter event (i.e. credit mode)	C3 – Sc4
	Unplanned outage information	D4 – Sc1
	Planned outage information	D4 – Sc3
16 (Meter)	Event notification confirmation	CDR&LC
	Event start confirmation	CDR&LC
	Event end confirmation	CDR&LC

Information in Transit		
Link (Destination)	Information	Reference
	HAN communication confirmation	C2 – Sc2
	Prepayment status receipt (from HAN Display Device)	C3 – Sc1, Sc2
17 (Field Tool)	Connects tool to meter (physical interaction)	B2 – Sc5
	Chooses to toggle electric service	B2 – Sc5
	Meter ID information	I1 – Sc1
	Report marginal coverage/"soft-registration"	I1 – Sc1
	Close out work order	I2 – Sc1
17 (Field Person)	Confirmation of turn on/off electric service	B2 – Sc5
	Meter ID match confirmation	I1 – Sc1
	Meter reading	I1 – Sc1
	Success of AMI system registration	I1 – Sc1
	Work order alert	I2 – Sc1
18 (Head End)	Non-electric meter read request	B4 – Sc1
	Reconfigure meter asset	I1 – Sc1
	Updated firmware	I3 – Sc1
	Execute firmware command	I3 – Sc1

Information in Transit		
Link (Destination)	Information	Reference
	Request HAN device ping	I3 – Sc2, Sc3
18 (AMI Meter Mgmt System)	Removal event	B3 – Sc1
	Re-installation event	B3 – Sc1
	Inversion event	B3 – Sc3
	Customer load detected event	B3 – Sc4
	Meter intrusion event	B3 – Sc5
	Meter location change or network disconnection event	B3 – Sc6
	Meter status	I1 – Sc1
	Meter service oder request	I2 – Sc2, Sc7, Sc8
	Confirmation of firmware update download	I3 – Sc1
19 (Data Portal)	*Non-electric meter read request*	*B4 – Sc1*
	Request non-electric meter data	*B4 – Sc1*
	Request non-electric meter event monitoring	*B4 – Sc5*
19 (Non Electric Utility)	*Non-electric meter read data*	*B4 – Sc1*
20 (AMI Network Mgmt System)	Non-electric meter read request	B4 – Sc1

Information in Transit		
Link (Destination)	Information	Reference
20 (Data Portal)		
21 (Head End)	Non-electric meter read request	B4 – Sc1
21 (AMI Network Mgmt System)	Meter event Activity record	S1 – Sc1, Sc3 S1 – Sc1
22 (Non Electric Meter)	Establish connection Meter read request Request meter event monitoring	B4 – Sc1 B4 – Sc1 B4 – Sc5
22 (Head End)	Connection established Meter read Non-electric meter event	B4 – Sc1 B4 – Sc1 B4 – Sc5, Sc6
23 (Non Electric Utility)	Identification of non electric meters where no data is received	B4 – Sc1
23 (MDMS)		
24 (MDMS)	Load shed control notification	CDR&LC
24 (DRAACS)	Load shed event end	CDR&LC

Information in Transit		
Link (Destination)	Information	Reference
25 (DRAACS)	Request load control	CDR&LC
25 (Grid Control Center)	Load shed report	CDR&LC
26 (Meter)	Event notification confirmation Event start confirmation Event end confirmation Customer HAN equipment response	CDR&LC CDR&LC CDR&LC C4 – Sc1
26 (Load Control Device)	Load control event notification Event start message Event end message Customer HAN equipment command	CDR&LC CDR&LC CDR&LC C4 – Sc1
27 (Customer)	*Displays event notification* *Event start message*	*CDR&LC* *CDR&LC*
27 (HAN Display Device)	*Opt out for optional events*	*CDR&LC*
28 (Customer)	*Displays event notification*	*CDR&LC*

Information in Transit		
Link (Destination)	Information	Reference
	Event start message	*CDR&LC*
28 (Load Control Device)	*Opt out for optional events*	*CDR&LC*
29 (Customer)		
29 (Utility Website)	*Customer energy data request*	*C2 – Sc3*
30 (Customer Rep)	*Prepay meter event report*	*C3 – Sc4*
30 (CIS)		
31(Customer)	*Payment request*	*C3 – Sc4*
31(Customer Rep)	*Prepayment request* *Disconnect request*	*C3 – Sc4* *C3 – Sc4*
32(Head End)	Power Quality data request Real-time data request (volts, watts, PF, etc.) Change of state command (i.e. Cap Bank On/Off)	D2 – Sc1 D2 – Sc3 D2 – Sc3
32(DMS)	Power Quality event	D2 – Sc1

Information in Transit		
Link (Destination)	Information	Reference
	Power Quality data response Real-time data response (volts, watts, PF, etc.)	D2 – Sc1 D2 – Sc3
33(Head End)		
33(Distribution Automation Node)	Change of state command (i.e. Cap Bank On/Off)	D2 – Sc3
34(CIS)	*DG enrollment response*	*D3 – Sc1*
34(DG Evaluation Team)	*DG enrollment request*	*D3 – Sc1*
35(AMI Meter Management System)	Meter service order	D4 – Sc1
35(Outage Mgmt System)		
36(AMI Meter Management System)		
36 (Field Person)	Meter service order	D4 – Sc1
37(Head End)	Power outage notification	D4 – Sc1

Information in Transit		
Link (Destination)	Information	Reference
	Power restoration notification Meter last gasp message Collector running on battery message Collector power restored	D4 – Sc1 D4 – Sc2 D4 – Sc2 D4 – Sc2
37(AMI Communications Network)		
38(MDMS)	Planned outage information	D4 – Sc3
38(Outage Mgmt System)	Power outage notification Power restoration notification	D4 – Sc1 D4 – Sc1
39(AMI Communications Network)	Meter last grasp message	D4 – Sc2
39(Meter)		
40(Outage Mgmt System)	Meter last grasp message Collector running on battery message Collector power restored	D4 – Sc2 D4 – Sc2 D4 – Sc2

Information in Transit		
Link (Destination)	Information	Reference
40(Head End)		
41 (AMI Forecasting)	Quantity and types of meters to order Meter change info	I1 – Sc1 I1 – Sc1
41 (CIS)	Customer notification of meter change information	I1 – Sc1
42 (Vendor)	Quantity and types of meters to order	I1 – Sc1
42 (AMI Forecasting)		
43 (AMI Meter Mgmt System)	Add meter asset request	I1 – Sc1
43 (Vendor)		
44 (Warehouse)	Expected meter arrival	I1 – Sc1
44 (AMI Meter Mgmt System)		
45 (Warehouse)	*Meter receipt confirmation*	*I1 – Sc1*
45 (Technicians)		

Information in Transit		
Link (Destination)	Information	Reference
46 (AMI Meter Mgmt System)	Meter receipt confirmation Meter test results Meter ready for deployment	I1 – Sc1 I1 – Sc1 I1 – Sc1
46 (Technicians)		
47 (AMI Meter Mgmt System)		
47 (Construction Maintenance Acct)	Dispatch of meter and communications equipment	I1 – Sc1
48 (Field Person)	*Issuance of meter*	*I1 – Sc1*
48 (Construction Maintenance Acct)		
49 (AMI Forecasting)	Meter inventory response	I1 – Sc1
49 (AMI Meter Mgmt System)	Request meter inventory	I1 – Sc1
50 (Workforce Mgmt)	Meter service order	I1 – Sc1

Information in Transit		
Link (Destination)	Information	Reference
50 (AMI Forecasting)		
51 (Construction Maintenance Acct)	*Meter service order*	*I1 – Sc1*
51 (Workforce Mgmt)		
52 (AMI Meter Mgmt System)	Close out meter service order	I2 – Sc1
52 (Enterprise Asset)	Meter service order	I2 – Sc1
53 (Workforce Mgmt)	*Meter service order*	*I2 – Sc1*
53 (Enterprise Asset)	*Close work order*	*I2 – Sc1*
54 (Field Tool)	Meter service order	I2 – Sc1
54 (Workforce Mgmt)	Work order results	I2 – Sc1
55 (CIS)		
55 (AMI Meter Mgmt System)	Meter service order request HAN device asset ID	I2 – Sc3 I3 – Sc2, Sc3

Information in Transit		
Link (Destination)	Information	Reference
56 (Dist Maintenance)		
56 (AMI Meter Mgmt System)	Meter testing service order request	I2 – Sc4
57 (AMI Network Mgmt System)		
57 (Outage Mgmt)	Outage record request Activity record	S1 – Sc1, Sc3 S1 – Sc1
58 (AMI Network Mgmt System)		
58 (Workforce Mgmt)	Work order request	S1 – Sc1, Sc3
59 (AMI Network Mgmt System)		
59 (Telecom Control Center)	Outage record request	S1 – Sc3