Xanthus
Consulting International

White Paper for NIST CSWG: Home Area Network (HAN) Cyber Security Requirements

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

Table of Contents

1. Interface Categories for Defining Security Requirements for Home Area Networks (HAN)

At the most basic level, ***security requirements*** for exchanging information among different systems for different business processes (as seen in Section 0) are stated as the need for confidentiality, integrity, and availability (CIA). But translating these basic requirements into feasibility and cost-effectiveness ***security measures*** must take into account the technical constraints, the environments, organizational issues, and primary security requirements of the interfaces. Therefore the interfaces that are used to exchange information need to be defined according to these constraints and issues.

For this reason, the interfaces related to HAN systems were identified and then categorized according to their major characteristics. These Interface Categories were then assessed against the DHS "*Catalog of Control System Security*" to provide guidelines for developing the appropriate security measures.

These security-related categories can be helpful as examples, guidelines, and/or checklists of security requirements to help utilities specify security requirements and to assist vendors and integrators as they design, implement, and maintain secure systems but in the end, actual security measures must reflect the real-world security requirements of specific implementations.

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

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

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

Requirement, Constraint, or Issue	Description
Cst-1: High requirement for confidentiality	which necessitates or strongly influences the types of security measures required.
Cst-1b: High requirement for privacy	which necessitates or strongly influences the types of security measures required.
Cst-2: High requirement for integrity and/or accuracy of data	which influences not only the types of typical security measures, but also necessitates strong accuracy and error checking.
Cst-3: High requirement for availability	which influences system design, network configuration, and procedures for achieving the necessary availability
Cst-4: *Low bandwidth of communications channels*	which limits the types of security measures which could be employed per channel.
Cst-5: *Microprocessor constraints on memory and compute capabilities*	which limits the types of security measures which could be employed.

Requirement, Constraint, or Issue	Description
Cst-6: *Wireless media*	which can pose certain types of additional security challenges.
Cst-7: *Immature or proprietary protocols*	which may not be adequately tested either against inadvertent compromises or deliberate attacks.
Cst-8: *Cross-organizational interactions*	which limit trust and compatibility of security policies and measures, including the use of out-sourced services and leased networks.
Cst-9: *Real-time operational requirements*	which entail short acceptable time latencies, and limit the choices for stopping or mitigating on-going attacks.
Cst-10: *Legacy end-devices and systems*	which limit the types, thoroughness, or effectiveness of different security measures which could be employed.
Cst-11: *Legacy communication protocols*	which limit the types, thoroughness, or effectiveness of different security measures which could be employed.
Cst-12: *Insecure locations*	which cannot be made more secure due to their physical environment or ownership.
Cst-13: *Key management for large numbers of devices*	which can limit the methods for deploying and revoking keys.
Cst-14: *Patch and update management constraints for sensitive devices*	which limits the frequency of updating security patches.
Cst-15: *Unknown or rapidly changing types of interactions*	which complicate the decisions on the types and severity of security threats and impacts.
Cst-16: *Environmental and physical access constraints*	which limit the types of security measures, particularly physical security.
Cst-21: *Sharing of known security vulnerabilities and security incidents limited by legal and/or regulatory factors*	which can cause vulnerabilities to perpetuate.
Cst-22: *Novel business functions with unknown ramifications from security breaches*	which can either lead to unwarranted, burdensome security measures or, more likely, inadequate security measures.

–

1.2 HAN/BAN Diagram

The Home Area Network (HAN) and Building Area Network (BAN) diagram used to identify the HAN interfaces is shown in Figure 1.

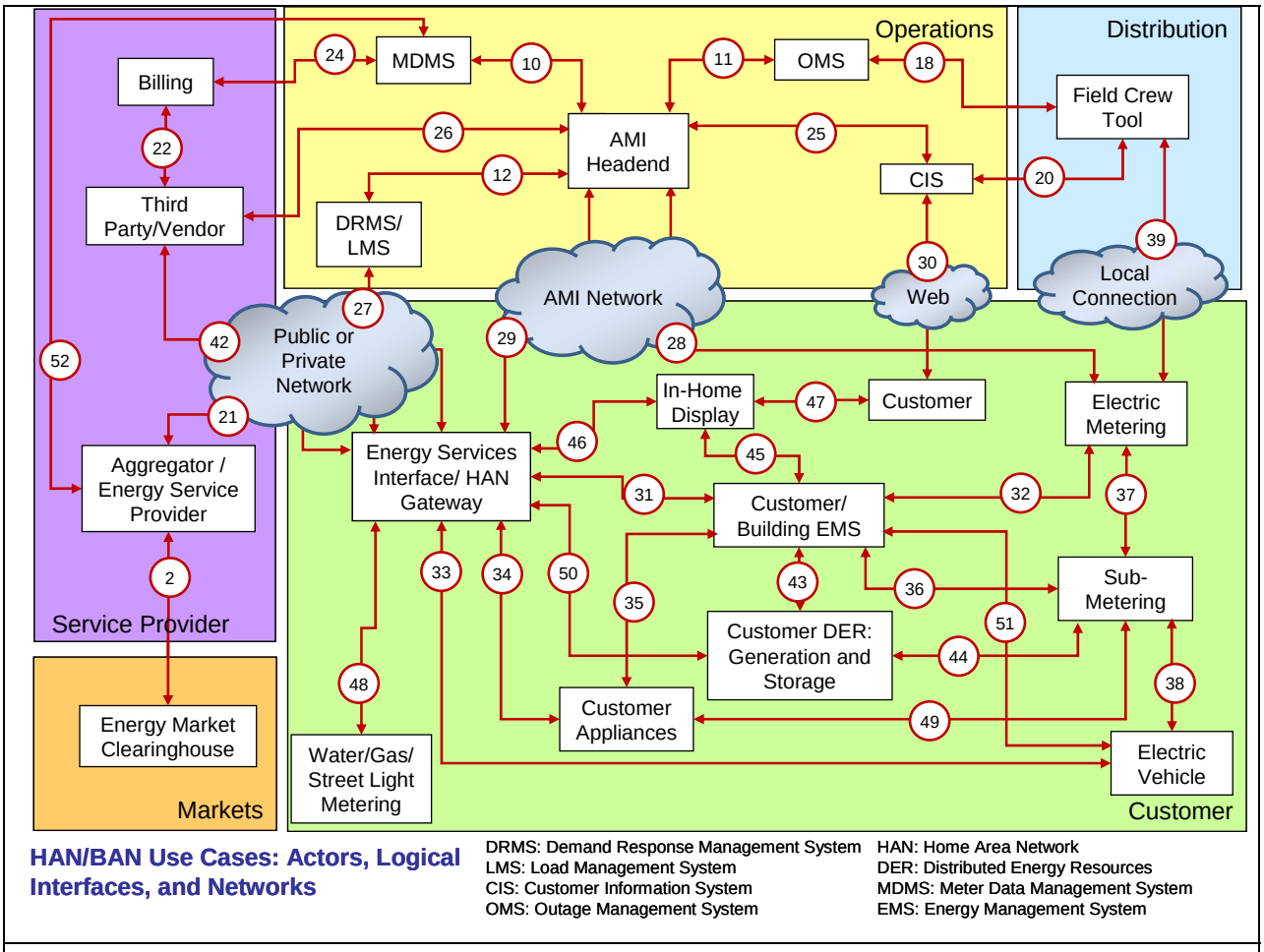

Figure 1: HAN/BAN System Actors, Logical Interfaces, and Networks

1.3 Security-Related Interface Categories

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

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

Table 2: Security-Related Interface Categories

Interface Categories	HAN Interfaces
1a. Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints – *E.g. Between transmission SCADA and substation equipment* – *Between distribution SCADA and high priority substation and pole-top equipment* – *Between SCADA and DCS within a power plant*	
1b. Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints – *E.g. Between distribution SCADA and lower priority pole-top equipment* – *Between pole-top IEDs and other pole-top IEDs* – *Between ESPs and Distributed Energy Resources and/or Load Controllers*	HAN 27 HAN-43
1c. Interface between control systems and equipment with high availability, without compute and/or bandwidth constraints – *E.g. Between transmission SCADA and substation automation systems*	
1d. Interface between control systems and equipment without high availability, without compute and/or bandwidth constraints – *E.g. Between distribution SCADA and backbone network-connected collector nodes for distribution pole-top IEDs*	
2. Interface between control systems in different organizations – *E.g. Between an RTO/ISO EMS and a utility energy management system* – *Between control systems and their vendors*	
3. Interface between control systems within the same organization – *E.g. multiple DMS systems belonging to the same utility* – *Between subsystems within DCS and ancillary control systems within a power plant*	
4. Interface between back office systems under common management authority – *E.g. Between a Customer Information System and a Meter Data Management System*	HAN 10 HAN 11 HAN 12 HAN 22 HAN 25
5. Interface between back office systems not under common management authority – *E.g. Between a third party billing system and a utility meter data management system*	HAN 23 HAN 24 HAN 52
6. Interface with B2B connections between systems usually involving financial or market transactions – *E.g. Between a Retail aggregator and an Energy Clearinghouse*	HAN 2
7. Interface between control systems and non-control systems – *E.g. between a Geographic Information System and a Load Management/Demand Response System*	
8. Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements – *E.g. between temperature sensor on a transformer and its receiver*	
9. Interface between sensor networks and control systems – *E.g. between a sensor receiver and the substation master*	

Interface Categories	HAN Interfaces
10. Interface between systems that use the AMI network – *E.g. Between MDMS and meters* – *Between LMS/DRMS and Customer EMS* – *Between DMS Applications and Customer DER* – *Between DMS Applications and DA Field Equipment*	HAN 26 HAN 28 HAN 29
11. Interface between systems that use customer (residential, commercial, and industrial) site networks such as HANs and BANs – *E.g. Between Customer EMS and Customer Appliances* – *Between Customer EMS and Customer DER* – *Between Energy Service Interface and PEV*	HAN 31 HAN 32 HAN 33 HAN 34 HAN 35 HAN 36 HAN 43 HAN 44 HAN 45 HAN 46 HAN 47 HAN 48 HAN 49 HAN 50 HAN 51
12. Interface between external systems and the customer site – *E.g. Between Customer and CIS Web site* – *Between Third Party and HAN Gateway* – *Between any non-metering entity and the Energy Services Interface (ESI) / HAN Gateway*	HAN 21 HAN 30 HAN 42
13. Interface between systems and mobile field crew laptops/equipment – *E.g. Between field crews and GIS* – *Between field crews and substation equipment*	
14. Interface between metering equipment – *E.g. Between sub-meter to meter* – *Between PEV meter and Energy Service Provider*	HAN 37 HAN 38
15. Interface between decision support systems – *E.g. Between WAMS and ISO/RTO*	
16. Interface between engineering/maintenance systems and control equipment – *E.g. Between engineering and substation relaying equipment for relay settings* – *Between engineering and pole-top equipment for maintenance* – *Within power plants*	
17. Interface between control systems and their vendors – *E.g. Between SCADA system and its vendor*	
18. Interface between security network/system management console and all networks and systems – *E.g. between a security console and network routers, firewalls, computer systems, and network nodes*	

1.4 Definition of Categories by Interface Characteristics

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

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

Requirements, Constraints, and Issues / Security-Related Categories for Interfaces	Cst-1a: High requirement for confidentiality	Cst-1b: High requirement for privacy	Cst-2: High requirement for integrity and/or accuracy of data	Cst-3: High requirement for availability	Cst-4: Low bandwidth of communications channels	Cst-5: Microprocessor constraints on memory and compute capabilities	Cst-6: Wireless media	Cst-7: Immature or proprietary protocols	Cst-8: Inter-organizational interactions	Cst-9: Real-time operational requirements	Cst-10: Legacy end-devices and systems	Cst-11: Legacy communication protocols	Cst-12: Insecure locations	Cst-13: Key management for large umbers of devices	Cst-14: Patch and update manage-ment constraints for sensitive devices	Cst-15: Unknown or rapidly changing types of interactions	Cst-16: Environmental and physical access constraints	Cst-21: Sharing of known security vulnerabilities and incidents	Cst-22: Novel business functions with unknown ramifications from security
1a. Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints			X	X	X	X	X			X	X	X		X	X		X		
1b. Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints			X		X	X	X			X	X	X		X	X		X		
1c. Interface between control systems and equipment with high availability, without compute and/or bandwidth constraints			X	X	X	X	X			X	X	X		X	X		X		
1d. Interface between control systems and equipment without high availability, without compute and/or bandwidth constraints			X		X	X	X			X	X	X		X	X	X			
2. Interface between control systems in different organizations			X	X					X	X		X		X	X				
3. Interface between control systems within the same organization			X	X						X		X			X				
4. Interface between back office systems under common management authority	X	X	X												X				
5. Interface between back office systems not under common management authority	X	X	X						X					X				X	
6. Interface with B2B connections between systems usually involving financial or market transactions	X	X	X	X					X	X				X		X		X	

Requirements, Constraints, and Issues / Security-Related Categories for Interfaces	Cst-1a: High requirement for confidentiality	Cst-1b: High requirement for privacy	Cst-2: High requirement for integrity and/or accuracy of data	Cst-3: High requirement for availability	Cst-4: Low bandwidth of communications channels	Cst-5: Microprocessor constraints on memory and compute capabilities	Cst-6: Wireless media	Cst-7: Immature or proprietary protocols	Cst-8: Inter-organizational interactions	Cst-9: Real-time operational requirements	Cst-10: Legacy end-devices and systems	Cst-11: Legacy communication protocols	Cst-12: Insecure locations	Cst-13: Key management for large umbers of devices	Cst-14: Patch and update manage-ment constraints for sensitive devices	Cst-15: Unknown or rapidly changing types of interactions	Cst-16: Environmental and physical access constraints	Cst-21: Sharing of known security vulnerabilities and incidents	Cst-22: Novel business functions with unknown ramifications from security
7. Interface between control systems and non-control systems	X	X	X	X				X	X						X	X			
8. Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements					X	X	X	X		X	X	X	X				X		
9. Interface between sensor networks and control systems			X		X	X	X	X		X	X	X		X			X		
10. Interface between systems that use the AMI network	X	X			X	X	X	X	X			X	X	X		X	X	X	
11. Interface between systems that use customer (residential, commercial, and industrial) site networks such as HANs	X					X	X	X	X	X			X	X		X	X		X
12. Interface between external systems and the customer site	X	X						X	X				X			X	X		X
13. Interface between systems and mobile field crew laptops/equipment	X		X		X		X	X		X			X	X	X		X	X	
14. Interface between metering equipment	X	X	X		X	X	X	X	X		X	X	X	X	X		X		
15. Interface between decision support systems			X						X	X									
16. Interface between engineering/maintenance systems and control equipment			X		X	X	X				X	X	X	X	X		X		
17. Interface between control systems and their vendors			X	X			X		X	X			X	X	X		X	X	
18. Interface between security network/system management console and all networks and systems	X		X	X						X				X	X	X	X	X	

2. General Security Requirements Applicable to Interface Categories

At one level, all security requirements are pertinent to all interfaces. But this is usually not economically or practically feasible – for actual implementations, a balance needs to be struck between

- The cost of implementing security measures (financial, maintenance effort, and performance impacts)
- And the cost of security breaches (financial, legal, and societal impacts).

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

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

2.1 Interface Categories Specifically Applicable to HAN Systems

Although business processes involving HAN systems can also impact many Interface Categories, as shown in Table 2, some Interface Categories are of particular importance:

- Interface Category 10: Interfaces that use the AMI network to the customer site
- Interface Category 11: Interface between systems that use customer (residential, commercial, and industrial) site networks such as HANs and BANs
- Interface Category 12: Interface between external systems and the customer site (via ESI / HAN Gateway)
- Interface Category 14: Metering Interfaces

2.2 General DHS Security Requirements

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

- Security Policies *(DHS-CSC 2.1)*
- Organizational Security *(DHS-CSC 2.2)*
- Personnel Security *(DHS-CSC 2.3)*
- System and Services Acquisition *(DHS-CSC 2.5)*
- Strategic Planning *(DHS-CSC 2.7)*
- Information and Document Management *(DHS-CSC 2.9)*

- System Development and Maintenance *(DHS-CSC 2.10)*
- Security Awareness and Training *(DHS-CSC 2.11)*
- Media Protection *(DHS-CSC 2.13)*
- Monitoring and Reviewing Control System Security Policy *(DHS-CSC 2.17)*
- Risk Management and Assessment *(DHS-CSC 2.18)*

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

- Physical and Environmental Security *(DHS-CSC 2.4)*
- Configuration Management *(DHS-CSC 2.6)*
- System and Communication Protection *(DHS-CSC 2.8)*
- Incident Response *(DHS-CSC 2.12)*
- System and Information Integrity *(DHS-CSC 2.14)*
- Access Control *(DHS-CSC 2.15)*
- Audit and Accountability *(DHS-CSC 2.16)*

3. Specific Security Requirements Applicable to Individual Interface Categories

3.1 Interface Category 1b: Interface between Control Systems and Equipment without High Availability, but with Compute and/or Bandwidth Constraints

In the HAN environment, the primary interactions that fall into Interface Category 1b are the monitoring and control between Energy Service Providers (ESPs) and the Distributed Energy Resources (DER) devices and/or loads that they are directly controlling. Specifically these interactions are those requiring tightly coupled exchanges between the ESPs and the devices, and so do not include Demand Response or other loosely-coupled interactions: those are covered in Category 12.

Therefore, the focus of this interface category is on the security requirements for *power system reliability*.

3.1.1 Interface Category 1b Characteristics

The following are the key characteristics of Interface Category 1b, although clearly some interactions will have only some of these characteristics, while others will have some of the other characteristics.

- Cst-2: High requirement for integrity and/or accuracy of data which influences not only the types of typical security measures, but also necessitates strong accuracy and error checking.
- Cst-3: High requirement for availability which influences system design, network configuration, and procedures for achieving the necessary availability
- Cst-4: *Low bandwidth of communications channels* which limits the types of security measures which could be employed per channel.
- Cst-5: *Microprocessor constraints on memory and compute capabilities* which limits the types of security measures which could be employed.
- Cst-9: *Real-time operational requirements* which entail short acceptable time latencies, and limit the choices for stopping or mitigating on-going attacks.
- Cst-10: *Legacy end-devices and systems* which limit the types, thoroughness, or effectiveness of different security measures which could be employed.
- Cst-11: *Legacy communication protocols* which limit the types, thoroughness, or effectiveness of different security measures which could be employed.
- Cst-12: *Insecure locations* which cannot be made more secure due to their physical environment or ownership.
- Cst-13: *Key management for large numbers of devices* which can limit the methods for deploying and revoking keys.
- Cst-14: *Patch and update management constraints for sensitive devices* which limits the frequency of updating security patches.
- Cst-16: *Environmental and physical access constraints* which limit the types of security measures, particularly physical security.
- Cst-18: *Lack of security-consciousness in personnel* which can cause inadvertent by-passing of security measures and can limit the number of properly trained personnel to manage and secure resources. This includes the lack of any security training of most customers.
- Cst-20: *Security budgetary constraints* which limit the development of good security policies and procedures, limit the security training of personnel, and constrain the types of security tools and services to properly monitor, test, and protect the resources.
- Cst-21: *Sharing of known security vulnerabilities and security incidents limited by legal and/or regulatory factors* which can cause vulnerabilities to perpetuate.
- Cst-23: *Lack of standards across interfaces* which can lead to ad hoc engineering, difficulty in testing between vendor systems, and increased likelihood of security holes.

3.1.2 Specific Interface Category 1b Issues

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

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

3.1.3 Security Control Requirements for Interface Category 1b

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

3.1.3.1 Physical and Environmental Security (DHS-CSC 2.4)

- Physical device access authorization *(DHS-CSC 2.4.3)*
  - *Authorization for device access should include identity establishment, role-based access control, and careful maintenance of access mechanisms such as keys and passwords.*

- Physical device access control *(DHS-CSC 2.4.4)*
  - *Locked boxes, electronic keys, and monitoring of locks for pole-top devices and other physically vulnerable equipment should be used*

3.1.3.2 Configuration management control (DHS-CSC 2.6)

- Configuration change control *(DHS-CSC 2.6.3)*
  - *Configuration management is critical for ensuring high reliability, and therefore changes should be very carefully controlled, including authorization through RBAC, testing of configuration changes for validity and unintended consequences, and the ability to "roll-back" any changes that do not meet the availability and/or other requirements.*
  - *Configurations can be physically changed and/or logically changed. Both types of changes should be controlled.*
  - *Configurations can address communication media (such as wireless configurations) as well as software configurations (such as parameter settings, database fields, and what software is in what system). Both types of configuration changes should be controlled.*
  - *Configurations can be changed temporarily to handle maintenance, repair, testing, etc. Configurations can also be changed permanently. Both types of configuration changes should be controlled.*

- Monitoring configuration changes *(DHS-CSC 2.6.4)*
  - *Communication configurations using meshed wireless systems to connect to field equipment should have continuous monitoring to ensure configurations are still valid, not compromised, nor denying service.*
  - *Monitoring configuration changes for systems not under the control of a single organization should ensure that all "stakeholders" receive (or are permitted to receive) notification of changes.*

- Configuration settings *(DHS-CSC 2.6.6)*
  - *Configuration settings should be restricted to meet the requirements, while still remaining flexible enough to meet unexpected requirements or emergency situations.*

3.1.3.3 System and Communication Protection (DHS-CSC 2.8)

- Denial of service protection *(DHS-CSC 2.8.5)*
  - *Although it can be difficult to protect against all denial of service attacks, Network and System Management (NSM) can provide intrusion detection and resource exhaustion detection so that mitigating actions can be rapidly invoked*
  - *IEC 62351-7 and other NSM technologies should be implemented to provide communication path monitoring to detect permanent and temporary path failures, as well as equipment and software failures*
  - *Redundancy of measurements can increase sources of data, so that denial from one source can be mitigated by access to the redundant source. Redundancy should be used where availability requirements are particularly stringent.*

  - *Redundancy of systems and equipment can increase the availability of visibility and software analysis. Redundancy, such as backup systems, backup data, or alternate analysis software, should be used where availability requirements are particularly stringent.*
  - *Wireless media can be particularly vulnerable to denial of service attacks, so mechanisms to, at a minimum, detect denial of service, and, for time-critical data, to provide alternate means to acquire this data either through redundancy or estimation, as appropriate.*

- Resource priority *(DHS-CSC 2.8.6)*
  - *For similar time latency requirements, higher priority data should be retrieved before lower priority data*
  - *During emergencies, priority of data should be strictly enforced*
  - *No critical data should be lost due to communication failures*

- Boundary protection *(DHS-CSC 2.8.7)*
  - *Except for SCADA systems themselves, access to SCADA data should be limited to one-way retrieval of data from a database or other site updated by the SCADA systems*
  - *Problems with one field device should not impact other field devices or SCADA monitoring of other field devices*

- Communication integrity *(DHS-CSC 2.8.8)*
  - *IEC 62351 security standards should be used to provide communication integrity of data*

- Cryptographic key establishment and management *(DHS-CSC 2.8.11)*
  - *Cryptography used for ensuring integrity should use key establishment and management techniques appropriate to legacy systems and communications, recognizing that direct access to certificates by field equipment is generally not feasible.*
  - *Key management for the field equipment and communication channels in this Interface Category has not been clearly developed as yet. This effort is underway in the IEC 62351 standards, and should be implemented when finalized.*
  - *"Bump-in-the-wire" technology may be used if no alternative is feasible*

- Transmission of security parameters *(DHS-CSC 2.8.14)*
  - *IEC 62351 security standards should be used to ensure the secure transmission of security parameters*

- Security roles (DHS-CSC 2.8.19)
  - *Role-Based Access Control (RBAC) should be used to establish precisely which individuals and applications play which roles, and what access authority each role has with respect to information being monitored and controlled over the interface.*

  - *Role access authorization should be per data item, not just by equipment or group of data. If legacy equipment and communication protocols do not permit this level of access control, then compensating security methods should be provided, such as limiting access within the SCADA system database.*

- Message authenticity *(DHS-CSC 2.8.20)*
  - *IEC 62351 security standards should be used to authenticate messages*

- Fail in known state *(DHS-CSC 2.8.24)*
  - *All equipment should revert to a previously-defined default condition upon loss of communications. This default condition should ensure minimal disruption to critical systems.*
  - *All failed equipment should not affect other equipment or disrupt critical systems.*

3.1.3.4 Incident Response (DHS-CSC 2.12)

- Continuity of operations plan *(DHS-CSC 2.12.2)*
  - *Power system operations incident planning should be extended to preparing not only for power system equipment and communications failures and overloads, but also for information infrastructure "failures" including inadvertent losses as well as deliberate attacks on information.*
  - *Critical information should be available from multiple sources if possible. If these additional sources have the information, but do not normally provide this information, then the incident plan should include methods for rapid access to these other sources. For example, meters can provide voltage information through the AMI system if normal access to DA equipment is not available.*
  - *Calculations should validate information and provide estimates for additional information*
  - *Power flow analysis of distribution systems (as well as transmission systems) should be available to provide estimated data as well as models for assessing the impact of incidents.*
  - *Control of power system and communications equipment should be included in the incident plan to allow remote actions to ameliorate the impact of incidents.*

- Continuity of operations roles and responsibilities *(DHS-CSC 2.12.3)*
  - *Power system operations incident planning should include the clear definition of roles to be played by all involved personnel*
  - *The incident plan should include the roles for field equipment (such as default settings on loss of remote communications)*
  - *Certain software applications and systems (such as Contingency Analysis, Demand Response, DER management, Direct Load Control, and other tools) should be in the incident plan for monitoring, assessing, and controlling equipment during emergency situations.*

- Incident response training, testing, and update *(DHS-CSC 2.12.4, .5, .6)*
  - *Incident plans that are only on paper are virtually useless. Periodic training and testing must also take place on the interfaces and equipment associated with this Interface Category – while not disrupting normal power system operations.*

- Incident handling *(DHS-CSC 2.12.7)*
  - *During an incident, for power system operations relying on the interfaces in this Interface Category, the key will be to utilize the incident plans, but also be flexible and aware enough to respond to unexpected or unplanned for situations. This will take training, access to information from multiple sources, and the ability to try innovative approaches if the planned approach is not succeeding.*

- Incident monitoring *(DHS-CSC 2.12.8)*
  - *Alarm and event monitoring should include not only equipment and power system events, but also security events. This A&E monitoring could be an expansion of SCADA operations*

- Incident reporting *(DHS-CSC 2.12.8)*
  - *All assessments of anomalies and/or alarms and events should be reported to the appropriate level so that any necessary correlations and corrective actions can take place*
  - *Often incidents are not reported outside a small group to avoid either embarrassment or the possibility that a different attacker would learn about it and use it again. However, great care should be taken not to use the latter excuse when the real reason is the former, since corrective action by other groups with similar vulnerabilities should also take place.*

- Alternate control center *(DHS-CSC 2.12.15)*
  - *Alternate control centers may be needed for transmission and distribution operational centers. The possibility for such an alternate center should be part of any design, even if not carried out in the near term.*

- Control system backup *(DHS-CSC 2.12.16)*
  - *All critical operational data should be backed up, using standard methods for ensuring that bad data is not written over the good data*

- Control system recovery and reconstitution *(DHS-CSC 2.12.17)*
  - *All operational systems should be designed so that authorized personnel can recover the previous state of the system after a deliberate attack or an inadvertent failure or mistake. This may include retrieving metering and other information from the customer sites as well as using backup data.*

3.1.3.5 System and Information Integrity (DHS-CSC 2.14)

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

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

- Security alerts and advisories *(DHS-CSC 2.14.5)*
  - *SCADA alarm and event handling of power system events should be extended to security alarm and events of information system events, with such alarms being directed to security personnel.*

- Software and information integrity *(DHS-CSC 2.14.7)*
  - *Communication protocols used over these interfaces should include authentication and integrity validation, such as is specified in the IEC 62351 standards for IEC 61850, IEC 60870-5, and DNP3.*
  - *Power system operations should be extended to assessing the validity of information received from the field equipment through multiple methods, such as reasonability assessment, redundancy, power flow-based estimations, etc.*
  - *For field equipment, monitoring of software changes, software halting, software restarts, etc. should be included in SCADA monitoring.*
  - *Availability of key information should be monitored and alarmed if not available within the required timeframe. This availability should include field measurements, software application execution results, and personnel inputs.*

- Information input restrictions *(DHS-CSC 2.14.9)*
  - *RBAC should be implemented to restrict input to authorized personnel and software applications.*

- Information input accuracy, completeness, validity, and authenticity *(DHS-CSC 2.14.10)*
  - *All input, whether from authorized personnel or software applications or inputs from field sensors, should be checked as much as feasible for accuracy, completeness, validity, and authenticity.*
  - *In particular, SCADA systems and field equipment should include reasonability checks, redundancy checking, and power-flow-based assessments of information accuracy*
  - *Software patches and upgrades should be validated very extensively before being implemented, particularly for sensitive field equipment*

- Error handling (DHS-CSC 2.14.11)
  - *All errors, whether associated with personnel inputs, software applications, communication errors, and/or sensor inputs, should be logged and the appropriate personnel notified*

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

3.1.3.6 Access Control (DHS-CSC 2.15)

- Access enforcement *(DHS-CSC 2.15.7)*
  - *Role-Based Access Control (RBAC) should be implemented per data item, not just by equipment or group of data. IEC 62351-8 (still under development) will specify these RBAC requirements specifically.*
  - *If legacy equipment and communication protocols do not permit this level of access control, then compensating security methods should be provided, such as limiting access within the SCADA system database.*

- Least privilege *(DHS-CSC 2.15.9)*
  - *Role-Based Access Control should use the concept of least privilege when designing roles and assigning individuals and applications to those roles. This is particularly important for sensitive information from field equipment.*

- Permitted actions without identification or authentication *(DHS-CSC 2.15.11)*
  - *Particularly for this Interface Category, it is recognized that authentication may not be implemented immediately due to legacy systems, communications, and equipment.*
  - *However, monitoring and logging of ALL control commands can be implemented "relatively" easily using existing SCADA and field equipment capabilities. Therefore, at least identification and logging of actions should be required.*

- Passwords (DHS-CSC 2.15.16)
  - *Passwords, using strong authentication, should be required for all access to field equipment, and should be used in conjunction with RBAC.*
  - *Default passwords should be changed immediately upon installation of systems and equipment.*

- Wireless access restrictions *(DHS-CSC 2.15.26)*
  - *Wireless systems have particular security vulnerabilities so that very clear guidelines should be developed to identify the types of information that can and cannot go over wireless media.*

3.1.3.7 Audit and Accountability (DHS-CSC 2.16)

- Auditable events *(DHS-CSC 2.16.2)*
  - *Power system events and all security-related events should be logged and timestamped for later analysis.*
  - *Categories and priorities of events should be established to ensure critical event information is provided to the right person or application for responding in a timely manner.*

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

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

Two types of security requirements are paramount in Interface Category 10:

- **Revenue metering integrity to ensure customer billing is accurate.**
- **Customer confidentiality and privacy, since some customer data may be transmitted across the AMI network.**

Interface Category 10 is focused on the interfaces that use the AMI network to access the customer site. These interfaces include those:

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

3.2.1 Interface Category 10 Characteristics

The following are the key characteristics of Interface Category 10, although clearly some interactions will have only some of these characteristics, while others will have some of the other characteristics.

- Cst-1a: High requirement for confidentiality and/or privacy which necessitates or strongly influences the types of security measures required.
- Cst-1b: High requirement for confidentiality and/or privacy which necessitates or strongly influences the types of security measures required.
- Cst-4: *Low bandwidth of communications channels* which limits the types of security measures which could be employed per channel.
- Cst-5: *Microprocessor constraints on memory and compute capabilities* which limits the types of security measures which could be employed.
- Cst-6: *Wireless media* which can pose certain types of additional security challenges.

- Cst-7: *Immature or proprietary protocols* which may not be adequately tested either against inadvertent compromises or deliberate attacks.
- Cst-8: *Cross-organizational interactions* which limit trust and compatibility of security policies and measures, including the use of out-sourced services and leased networks.
- Cst-11: Legacy communication protocols which limit the types, thoroughness, or effectiveness of different security measures which could be employed.
- Cst-12: *Insecure locations* which cannot be made more secure due to their physical environment or ownership.
- Cst-13: *Key management for large numbers of devices* which can limit the methods for deploying and revoking keys.
- Cst-15: *Unknown or rapidly changing types of interactions* which complicate the decisions on the types and severity of security threats and impacts.
- Cst-16: *Environmental and physical access constraints* which limit the types of security measures, particularly physical security.
- Cst-21: *Sharing of known security vulnerabilities and security incidents limited by legal and/or regulatory factors* which can cause vulnerabilities to perpetuate.

3.2.2 Specific Interface Category 10 Issues

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

- Most information from the customer must be treated as confidential and/or private.
- Integrity of metering data is clearly important in general, but alternate means for retrieving and/or validating it can be used, such as requesting it again or even rolling a truck.
- Availability is generally low across AMI networks since they are not designed for real-time interactions or rapid request-response requirements.
- Volume of traffic across AMI networks must be kept low to avoid denial of service situations
- Meters are constrained in their compute capabilities, primarily to keep costs down, which may limit the types and layers of security which could be applied.
- Revenue-grade meters must be certified, so that patches and upgrades require extensive testing and validation
- Meshed wireless communication networks are often used, which can present challenges related to wireless availability as well as on throughput and configurations.
- Key management of millions of meters and other equipment will pose significant challenges that have not yet been addressed as standards

- Due to the relatively new technologies used in AMI networks, communication protocols have not yet stabilized as accepted standards, nor have their capabilities been proven through rigorous testing.
- AMI networks span across organizations between utilities with corporate security requirements and customers with no or limited security capabilities or understandings.
- Utility-owned meters are in physically insecure locations that are not under utility control, limiting physical security
- Many possible future interactions across the AMI network are still being designed, or are just being speculated about, or have not yet been conceived
- Customer reactions to AMI systems and capabilities are as yet unknown, and some may fear or reject the intrusion of such "Big Brother" systems.

3.2.3 Security Control Requirements for Interface Category 10

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

3.2.3.1 Physical and Environmental Security (DHS-CSC 2.4)

- Physical access control *(DHS-CSC 2.4.3)*
  - *Since meters cannot prevent access by customers and other people, very strong cryptographic technologies should be implemented for registers, databases, and other sensitive material within the meter*
  - *In particular, cryptographic keys should be stored encrypted and non-contiguously, and should never be copied into RAM.*
- Monitoring physical access *(DHS-CSC 2.4.4)*
  - *Given the vulnerability of meters to physical access, monitoring physical access should be designed into the meter and the AMI system*
  - *Tamper detection has been a meter requirement for many years. Using this capability can also help monitor physical access.*
  - *AMI network nodes should also be monitored for physical access*
  - *Locks, limited physical access, and physical means should be used for AMI headend systems*

3.2.3.2 Configuration Management (DHS-CSC 2.6)

- Configuration change control *(DHS-CSC 2.6.3)*
  - *Configuration management is critical for ensuring high reliability, and therefore changes should be very carefully controlled, including authorization through RBAC, testing of configuration changes for validity and unintended consequences, and the*

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

- *Configurations can be physically changed and/or logically changed. Both types of changes should be controlled.*
- *Configurations can address communication media (such as wireless configurations) as well as software configurations (such as parameter settings, database fields, and what software is in what system). Both types of configuration changes should be controlled.*
- *Configurations can be changed temporarily to handle maintenance, repair, testing, etc. Configurations can also be changed permanently. Both types of configuration changes should be controlled.*

- Monitoring configuration changes *(DHS-CSC 2.6.4)*
  - *Both meters and AMI network nodes should be monitored for configuration changes.*
  - *In particular, the connection path between the meter and the AMI Headend should be monitored so that any changes that are outside "normal" path variations in any meshed portions of the network can be alarmed.*
  - *Inability to access a meter previously accessible should be alarmed after a "reasonable" timeframe.*
  - *Communication configurations using meshed wireless systems to connect to field equipment should have continuous monitoring to ensure configurations are still valid, not compromised, nor denying service.*
  - *Monitoring configuration changes for systems not under the control of a single organization should ensure that all "stakeholders" receive (or are permitted to receive) notification of changes.*

- Access restrictions for configuration changes *(DHS-CSC 2.6.5)*
  - *RBAC should be used to restrict access to making configuration changes to the AMI network to authorized personnel and software applications*

- Configuration settings *(DHS-CSC 2.6.6)*
  - *RBAC should be used to restrict access to making changes to settings and parameters of the AMI network to authorized personnel and software applications*
  - *RBAC should also be used to restrict access to making setting and parameter changes to meters*

- Configuration for least functionality *(DHS-CSC 2.6.7)*
  - *AMI networks should not (yet) be strictly restricted to least functionality since there are expectations that they could be used for many different and unknown functions. However, some restrictions should limit obviously out-of-scope functions.*
  - *That said, new functions should be added to AMI networks with care not to unnecessarily impact the performance and security of existing functions.*

- *Metering interfaces should be strictly limited to known metering functions*

- Factory default authentication management *(DHS-CSC 2.6.10)*
  - *Meters should have factory-provided default certificates to secure them during shipment. These certificates should be changed to utility-provided certificates upon arrival and warehousing. Another certificate change should occur when installed in the field.*
  - *AMI network components, including the AMI headend should also have their factory-provided default certificates and/or passwords changed immediately upon installation.*

3.2.3.3 System and Communication Protection (DHS-CSC 2.8)

- Security function isolation *(DHS-CSC 2.8.3)*
  - *Many "security functions" are actually part of the normal AMI network and system management in which AMI nodes, communications, and end devices are monitored for anomalous events, and actions taken to mitigate problems, whether deliberately or inadvertently caused. Therefore, these security functions should not be isolated from normal operations.*
  - *Some security functions, such as establishing access controls, key management, and information prioritization and flow control, should be separated from operational functions.*

- Denial of service protection *(DHS-CSC 2.8.5)*
  - *Although availability security requirements should not be high for any individual interaction across an AMI system, the overall availability of the AMI should be relatively high. Therefore, any critical AMI component, such as the AMI headend or backbone communications, should be designed with redundancy and/or other configurations to enhance availability.*
  - *Where availability requirements are more important, the AMI system could provide redundancy of equipment, alternate paths, battery backup, and other methods for improving availability.*
  - *Network and System Management (NSM) should provide intrusion detection and resource exhaustion detection, with notification of these events securely provided to appropriate personnel and/or systems.*
  - *IEC 62351-7 and other NSM technologies should be implemented on the AMI networks to provide communication path monitoring to detect permanent and temporary path failures, as well as equipment and software failures*
  - *Redundancy of measurements, where these are available, can increase sources of data and thus minimize the impact of denial-of-service events. Although not generally feasible for individual metering, redundant measurements for distribution system monitoring could be provided.*

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

- Resource priority *(DHS-CSC 2.8.6)*
  - *Priority of different types of data should be clearly defined and implemented on AMI systems*
  - *For similar time latency requirements, higher priority data should be retrieved before lower priority data*
  - *During emergencies, priority of data should be strictly enforced, including the rejection of all low priority data*
  - *No critical data should be lost due to communication failures, so that it can be retrieved at a later time with no loss of accuracy.*

- Boundary protection *(DHS-CSC 2.8.7)*
  - *AMI system boundaries should be clearly defined, including at least separate boundaries for metering information, for power system operational information, for security management information, for sensitive customer information, and for non-utility "public" information*
  - *These AMI system boundaries should be protected as appropriate and as feasible through physical separation, virtual separation, layered security, RBAC, and/or other security mechanisms.*
  - *Information traffic across these boundaries should be avoided*
  - *Any cross-boundary interactions should be monitored and logged, with unexpected interactions causing alarms*
  - *Access to data transmitted across the AMI system should be limited to authorized systems through RBAC procedures as much as feasible, recognizing that field locations of AMI components must be considered untrusted*
  - *Information from the Home Area Network (HAN) should always be treated as untrusted, with strict constraints imposed on what types of data can be exchanged between the HAN and the AMI system. Unnecessary interactions should be avoided.*
  - *Security problems within one area of the AMI system should not impact other areas of the AMI system*
  - *Information crossing any boundary should be validated for reasonability, expected accuracy, and possible modification, with anomalies timestamped and logged, and/or alarmed.*

- Communication integrity *(DHS-CSC 2.8.8)*
  - *For information with high integrity requirements, authentication of the source of the information should be used. This authentication may or may not require encryption of the information.*

- *All information transmitted across an AMI system should be validated to the appropriate level of accuracy, using VEE practices where appropriate or other similar reasonability and validity checking methods.*
- *Given the untrusted nature of the AMI system, critical information should always have backup or redundant means of access, including alternate communication paths (e.g. truck-roll), alternate sources (e.g. secondary voltage sources), or methods for estimation (e.g. VEE or State Estimation function).*

- Communication confidentiality *(DHS-CSC 2.8.9)*
  - *For information with high confidentiality requirements, cryptographic mechanisms should be used, as defined in appropriate AMI security standards*
  - *The AMI system and its components should be designed to handle the additional compute and communication traffic requirements to utilize the recommended cryptographic technologies.*

- Trusted path (DHS-CSC 2.8.10)
  - *Since AMI systems cannot provide completely trusted paths nor independent certificate management for field devices, in addition to establishing best practices for such paths, all information should be validated and checked for confidentiality compromises, and certain sensitive data should checked periodically against alternate sources of this data.*

- Cryptographic key establishment and management *(DHS-CSC 2.8.11)*
  - *Cryptography used for sensitive information should use key establishment and management techniques appropriate to meters, field equipment, and bandwidth-limited communications, recognizing that direct access to certificates by field equipment is generally not feasible.*
  - *Key management for large numbers of field equipment and bandwidth-limited communication channels has not been developed as yet. This effort is underway in the IEC 62351 standards, and should be implemented when finalized.*
  - *"Bump-in-the-wire" technology could be used where feasible*

- Transmission of security parameters *(DHS-CSC 2.8.14)*
  - *Security standards for AMI systems, when available, should be used to ensure the secure transmission of security parameters. These could include the ANSI C12.22, and IEC standards*

- Security roles (DHS-CSC 2.8.19)
  - *Role-Based Access Control (RBAC) should be used to establish precisely which individuals and applications play which roles, and what access authority each role has with respect to information being monitored and controlled over the interface.*
  - *Role access authorization should be per data item, not just by equipment or group of data.*

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

- Message authenticity *(DHS-CSC 2.8.20)*
  - *IEC 62351 security standards should be used to authenticate messages*

- Fail in known state *(DHS-CSC 2.8.24)*
  - *All equipment should revert to a previously-defined default condition upon loss of communications. This default condition should ensure minimal disruption to critical systems*
  - *All failed equipment should not affect other equipment or disrupt critical systems.*

- Confidentiality of information at rest *(DHS-CSC 2.8.28)*
  - *AMI system components will contain information that must remain confidential and/or private. These components should use cryptographic techniques to ensure the confidentiality of this information.*

3.2.3.4 Incident Response (DHS-CSC 2.12)

- Continuity of operations plan *(DHS-CSC 2.12.2)*
  - *Critical information should be available from multiple sources if possible. If these additional sources have the information, but do not normally provide this information, then the incident plan should include methods for rapid access to these other sources. For example, meters can provide voltage information through the AMI system if normal access to DA equipment is not available.*

- Continuity of operations roles and responsibilities *(DHS-CSC 2.12.3)*
  - *AMI system incident planning should include the clear definition of roles to be played by all involved personnel*
  - *The incident plan should include the roles for field equipment upon the occurrence of an incident. For instance, all equipment should have default settings or modes in case of the loss of communications beyond expected limits.*
  - *Certain software applications and systems (such as tamper detection, revenue protection, confidentiality monitoring, and other tools) should be included the incident plan for monitoring, assessing, and controlling equipment during emergency situations.*

- Incident response training, testing, and update *(DHS-CSC 2.12.4, .5, .6)*
  - *Incident plans that are only on paper are virtually useless. Periodic training and testing must also take place on the interfaces and equipment associated with this Interface Category – while not disrupting normal power system operations or compromising metering confidentiality.*
  - *Power system training simulators and testing tools can help train personnel in handling security-related incidents*

- Incident handling *(DHS-CSC 2.12.7)*
  - *Unlike some other systems, control systems cannot just be shut down during an incident – they must be kept running.*
  - *During an incident, the key will be to utilize the incident plans, but also be flexible and aware enough to respond to unexpected or unplanned for situations. This will take training, access to information from multiple sources, and the ability to try innovative approaches if the planned approach is not succeeding.*
  - *AMI systems, if used to send demand response or other signals to customer-based DER equipment, should be designed to expect equipment and system failures, so that critical DER equipment can continue to perform as needed to help maintain power system reliability.*

- Incident monitoring *(DHS-CSC 2.12.8)*
  - *All anomalies should be monitored and assessed, both automatically, and if warranted, brought to the attention of a security operator. Sometimes what appears to be innocuous to a power system operator or customer representative could be a critical signal of a possible security attack to a security operator*
  - *Alarm and event monitoring of systems and equipment connected to the AMI system should include not only equipment and power system events, but also security events. This A&E monitoring could be an expansion of AMI system management.*
  - *All alarm and events should be assessed for security-related concerns as well as power system operational concerns or customer-related concerns.*
  - *Alarm and event logs should contain a synchronized timestamp that is appropriately accurate so that correlations across wide spread systems can take place*
  - *For some types of critical situations, the state and measurements of the power system and/or the information system should be captured and saved periodically (every 2-10 seconds for critical power system states), then discarded after a while if no incident occurs. If an incident does occur, then the sequence of periodic saved information can be critical to understanding what happened.*

- Incident reporting *(DHS-CSC 2.12.8)*
  - *All assessments of anomalies and/or alarms and events should be reported to the appropriate level so that any necessary correlations and corrective actions can take place*
  - *Often incidents are not reported outside a small group to avoid either embarrassment or the possibility that a different attacker would learn about it and use it again. However, great care should be taken not to use the latter excuse when the real reason is the former, since corrective action by other groups with similar vulnerabilities should also take place.*

- Alternate control center *(DHS-CSC 2.12.15)*
  - *Alternate control centers may be needed by AMI systems as their functionality and criticality grow. The possibility for such an alternate center should be part of any design, even if not carried out in the near term.*

- Control system backup *(DHS-CSC 2.12.16)*
  - *All AMI system data should be backed up, using standard methods for ensuring that bad data is not written over the good data*

- Control system recovery and reconstitution *(DHS-CSC 2.12.17)*
  - *All AMI systems should be designed so that authorized personnel can recover the previous state of the system after a deliberate attack or an inadvertent failure or mistake. This may include retrieving metering and other information from the customer sites as well as using backup data.*

3.2.3.5 System and Information Integrity (DHS-CSC 2.14)

- System monitoring tools and techniques *(DHS-CSC 2.14.4)*
  - *AMI systems should include intrusion detection for all components, including meters, network nodes, and the AMI headend. Intrusions should be reported using the AMI system monitoring capabilities to identify and alarm security events.*
  - *If communication and equipment constraints do not permit this level of event monitoring, then compensating security methods should be provided, such as additional monitoring of equipment status to detect shut-downs, restarts, and physical access.*

- Security alerts and advisories *(DHS-CSC 2.14.5)*
  - *AMI system alarm and event handling of events should be extended to security alarm and events of information system events, with such alarms being directed to security personnel.*

- Software and information integrity *(DHS-CSC 2.14.7)*
  - *Communication protocols used over the AMI system should include authentication and integrity validation.*
  - *AMI systems should assess the validity of information received from the field equipment through multiple methods, such as reasonability assessment, redundancy, power flow-based estimations, etc.*
  - *AMI systems that monitor field equipment should also monitor software changes, software halting, software restarts, etc.*
  - *Availability of key information should be monitored and alarmed if not available within the required timeframe. This availability should include field measurements, software application execution results, and personnel inputs.*

- Information input restrictions *(DHS-CSC 2.14.9)*
  - *RBAC should be implemented to restrict input to authorized personnel and software applications.*
  - *All information received from field locations should be strictly limited to authorized personnel, potentially with two-step authentication for critical interactions.*

- Information input accuracy, completeness, validity, and authenticity *(DHS-CSC 2.14.10)*
  - *All input, whether from authorized personnel or software applications or inputs from field sensors, should be checked as much as feasible for accuracy, completeness, validity, and authenticity.*
  - *In particular, AMI systems should include reasonability checks, redundancy checking, and revenue protection assessments of information accuracy*
  - *Software patches and upgrades should be validated very extensively before being implemented, particularly for sensitive field equipment*

- Error handling (DHS-CSC 2.14.11)
  - *All errors, whether associated with personnel inputs, software applications, communication errors, and/or sensor inputs, should be logged and the appropriate personnel notified*
  - *Categorization and prioritization of errors should be provided to ensure the most important errors and alarms are sent to the appropriate personnel in a timely manner.*

3.2.3.6 Access Control (DHS-CSC 2.15)

- Access enforcement *(DHS-CSC 2.15.7)*
  - *Role-Based Access Control (RBAC) should be implemented per data item, not just by equipment or group of data.*
  - *If legacy equipment and communication constraints do not permit this level of access control, then compensating security methods should be provided, such as limiting access within the AMI system database.*

- Least privilege *(DHS-CSC 2.15.9)*
  - *Role-Based Access Control should use the concept of least privilege when designing roles and assigning individuals and applications to those roles. This is particularly important for sensitive information from field equipment.*

- Permitted actions without identification or authentication *(DHS-CSC 2.15.11)*
  - *Monitoring and logging of ALL control commands should be implemented, even during emergency overrides. Therefore, at least identification and logging of actions should be required.*

- Passwords (DHS-CSC 2.15.16)
  - *Passwords, using strong authentication, should be required for all access AMI components, and should be used in conjunction with RBAC.*
  - *Default passwords should be changed immediately upon installation of systems and equipment.*

- Wireless access restrictions *(DHS-CSC 2.15.26)*

- *Wireless systems have particular security vulnerabilities so that very clear guidelines should be developed to identify the security measures to be implemented and the types of information that are permitted and not permitted to go over wireless media.*

3.2.3.7 Audit and Accountability (DHS-CSC 2.16)

- Auditable events *(DHS-CSC 2.16.2)*
  - *Power system events, customer-based events, and all security-related events should be logged and timestamped for later analysis.*
  - *Categories and priorities of events should be established to ensure critical event information is provided to the right person or application for responding in a timely manner.*

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

3.3 Interface Category 11: Interfaces among systems that use customer (residential, commercial, and industrial) site networks such as HANs and BANs

Two types of security requirements are paramount in Interface Category 11 – interactions within the HAN:

- **Power system reliability involving Distributed Energy Resources (generation, storage, and to some degree, load). With increasing amounts of DER at customer sites, the reliability of the power grid is increasingly impacted by the security of the HAN systems which connect and manage these DER devices.**
- **Customer confidentiality and privacy, since so many stakeholders have some degree of access to the HAN. This stakeholder access must be well managed.**

Interface Category 11 is focused on the interfaces within the customer site: among and between systems that use customer (residential, commercial, and industrial) site networks such as HANs and BANs. These interfaces include those:

- Between the ESI/HAN Gateway and the Customer EMS, such as Demand Response signals, load management signals, DER management settings and controls, and registration of appliances and equipment
- Between the ESI/HAN Gateway and Customer DER, such as PV inverters, battery storage, wind turbines, fuel cells, etc.

- Between the Customer EMS and Customer Appliances, such as thermostats, HVAC systems, electric driers,
- Between Customer EMS and Customer DER
- Between ESI/HAN Gateway and PEV

3.3.1 Interface Category 11 Characteristics

The following are the key characteristics of Interface Category 11, although clearly some interactions will have only some of these characteristics, while others will have some of the other characteristics.

- Cst-1a: High requirement for confidentiality which necessitates or strongly influences the types of security measures required.
- Cst-5: *Microprocessor constraints on memory and compute capabilities* which limits the types of security measures which could be employed.
- Cst-6: *Wireless media* which can pose certain types of additional security challenges.
- Cst-7: *Immature or proprietary protocols* which may not be adequately tested either against inadvertent compromises or deliberate attacks.
- Cst-8: *Cross-organizational interactions* which limit trust and compatibility of security policies and measures, including the use of out-sourced services and leased networks.
- Cst-9: Real-time operational requirements, which entail short acceptable time latencies, and limit the choices for stopping or mitigating on-going attacks.
- Cst-12: *Insecure locations* which cannot be made more secure due to their physical environment or ownership.
- Cst-13: *Key management for large numbers of devices* which can limit the methods for deploying and revoking keys.
- Cst-15: *Unknown or rapidly changing types of interactions* which complicate the decisions on the types and severity of security threats and impacts.
- Cst-16: *Environmental and physical access constraints* which limit the types of security measures, particularly physical security.
- Cst-22: *Novel business functions with unknown ramifications from security breaches* which can either lead to unwarranted, burdensome security measures or, more likely, inadequate security measures.

3.3.2 Specific Interface Category 11 Security-Related Issues

The security-related issues for this intra-customer-site HAN Interface Category include the following:

- Some information exchanged among different appliances and systems must be treated as confidential to ensure that an unauthorized third party does not gain access to it. For instance, energy usage statistics from the customer site that are sent through the ESI/HAN gateway must be kept confidential from other appliances whose vendors may want to scavenge this information for marketing purposes.
- Integrity of data is clearly important in general, but since so many different types of interactions are taking place, the integrity requirements will need to be specific to the particular application
- Availability is generally low across HAN networks since most interactions are not needed in real-time. Even DER generation and storage devices have their own integrated controllers which are normally expected to run independently of any direct monitoring and control, and must have "default" modes of operation to avoid any power system problems.
- Bandwidth is not generally a concern, since most HAN network media will be local wireless (e.g. WiFi, ZigBee, Bluetooth) or power line (e.g. HomePlug). The latter may be somewhat bandwidth limited, but can always be replaced by cable or wireless if the bandwidth is needed.
- Some HAN devices are constrained in their compute capabilities, primarily to keep costs down, which may limit the types and layers of security which could be applied.
- Wireless communication networks are expected to be used within the HAN, which could present some challenges related to wireless configuration and security, primarily due to the fact that most HANs will not have security experts managing these systems. For instance, if available security measures are not properly set, the HAN security could be compromised by any one of the internal devices as well as by external entities searching for these insecure HANs.
- Key management of millions of devices within millions of HANs will pose significant challenges that have not yet been addressed as standards
- Due to the relatively new technologies used in HAN networks, communication protocols have not yet stabilized as accepted standards, nor have their capabilities been proven through rigorous testing. For instance, the Smart Energy Profile (SEP v2) is not expected to be widely available or stable for at least a couple of years.
- HAN networks will be accessible by many different vendors and organizations with unknown corporate security requirements and equally variable degrees and types of security solutions. Even if one particular interaction is "secure", in aggregate these multiplicity of interactions may not be secure.
- Some HAN devices may be in physically insecure locations, thus limiting physical security. Even those presumably "physically secure" within a home are vulnerable to inadvertent situations such as poor maintenance and mis-use, as well as break-ins and theft.
- Many possible future interactions within the HAN environment are still being designed, or are just being speculated about, or have not yet been conceived

3.3.3 Security Control Requirements for Interface Category 11

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

3.3.3.1 Physical and Environmental Security (DHS-CSC 2.4)

- Physical access control *(DHS-CSC 2.4.3)*
  - *Since HAN devices cannot prevent access by customers and other people, very strong cryptographic technologies should be implemented for "sensitive" equipment with high security confidentiality and integrity requirements*
  - *In particular, cryptographic keys should be stored encrypted and non-contiguously, and should never be copied into RAM.*

- Monitoring physical access *(DHS-CSC 2.4.4)*
  - *Given the vulnerability of HAN devices to physical access, all sensitive devices (or their controllers) should, at a minimum, self-monitor for inappropriate physical access, and when possible, log the event and take other appropriate action such as shutting off.*
  - *Tamper detection has been a metering requirement for many years. For some sensitive devices, the sensors and techniques used for detecting meter tampering could be used. For instance, PEV charging stations should detect any attempts of tampering with the connectors, internal meters, and controllers.*
  - *HAN network nodes should also be monitored and logged for physical access, such as unplugging connectors or restarting components.*

3.3.3.2 Configuration Management (DHS-CSC 2.6)

- Configuration change control *(DHS-CSC 2.6.3)*
  - *HAN configuration management is critical for ensuring appropriate availability and integrity. The most likely configuration changes will occur when new HAN devices are added or moved. Although ultimately the HAN configuration is the responsibility of the customer, all HAN devices and HAN communication nodes should include testing of configuration changes for validity and unintended consequences, and the ability to "roll-back" or "undo" any changes that do not meet the permissibility, availability and/or other requirements.*

- Monitoring configuration changes *(DHS-CSC 2.6.4)*
  - *Configurations can be physically changed and/or logically changed. Both types of changes should be monitored.*
  - *Configurations can address communication media (such as wireless configurations) as well as software configurations (such as parameter settings, database fields, and what software is in what system). Both types of configuration changes should be monitored.*

  - *Configurations can be changed temporarily to handle maintenance, repair, testing, etc. Configurations can also be changed permanently. Both types of configuration changes should be monitored.*
  - *Monitoring configuration changes for systems should ensure that all authorized "stakeholders" receive (or are permitted to receive) notification of changes.*

- Access restrictions for configuration changes *(DHS-CSC 2.6.5)*
  - *RBAC should be used to restrict access to making configuration changes to the HAN network to authorized personnel (e.g. customer) and software applications.*

- Configuration settings *(DHS-CSC 2.6.6)*
  - *RBAC should be used to restrict access to making changes to settings and parameters of the HAN network to authorized personnel (e.g. customer) and software applications.*
  - *RBAC should also be used to restrict access to making setting and parameter changes to meters*

- Factory default authentication management *(DHS-CSC 2.6.10)*
  - *"Sensitive" HAN devices, such as PEV charger meters and including HAN communication nodes, should have factory-provided default certificates to secure them during shipment. These certificates should be changed when installed in the field.*

3.3.3.3 System and Communication Protection (DHS-CSC 2.8)

- Security function isolation *(DHS-CSC 2.8.3)*
  - *Many "security functions" are actually part of the normal HAN network and system management in which HAN nodes, communications, and end devices are monitored for anomalous events, and actions taken to mitigate problems, whether deliberately or inadvertently caused. Therefore, these security functions should not be isolated from normal operations.*
  - *Some security functions, such as establishing access controls, key management, and information prioritization and flow control, should be separated from operational functions.*

- Denial of service protection *(DHS-CSC 2.8.5)*
  - *Although availability security requirements are not generally very stringent on HAN networks, for those devices where availability is critical, certain protection such as redundancy, backup, alternate sources of power, alternate sources of data, etc., could be used.*
  - *Network and System Management (NSM) should provide intrusion detection and resource exhaustion detection, with notification of these events securely provided to appropriate personnel and/or systems.*

- *IEC 62351-7, SNMP, and other NSM technologies should be implemented on the HAN networks to provide communication path monitoring to detect permanent and temporary path failures, as well as equipment and software failures*
- *Wireless media can be particularly vulnerable to denial of service attacks, so mechanisms should be provided to, at a minimum, detect denial of service, and, for time-critical data, to provide alternate means to acquire this data either through redundancy or estimation, as appropriate.*

- Resource priority *(DHS-CSC 2.8.6)*
  - *Priority of different types of data should be clearly defined and implemented on HAN systems.*
  - *For similar time latency requirements, higher priority data should be retrieved before lower priority data.*
  - *During emergencies, priority of data should be strictly enforced, including the rejection of all low priority data.*
  - *No critical data should be lost due to communication failures, so that it can be retrieved at a later time with no loss of accuracy.*

- Boundary protection *(DHS-CSC 2.8.7)*
  - *HAN systems may have separate networks for different types of devices with different configurations and/or performance requirements. For multi-network HAN systems, boundaries should be clearly defined, including at least separate boundaries for any sub-metering information, for devices requiring tightly-coupled management (e.g. DER control), for devices needing only loosely-coupled interactions (e.g. HVAC), for security management information, for sensitive customer information, and for "public" information*
  - *These HAN system boundaries should be protected as appropriate and as feasible through physical separation, virtual separation, layered security, RBAC, and/or other security mechanisms.*
  - *Information traffic across these boundaries should be avoided.*
  - *Any cross-boundary interactions should be monitored and logged, with unexpected interactions causing alarms*
  - *Access to data transmitted across the HAN system boundaries should be limited to authorized systems through RBAC procedures as much as feasible.*
  - *Security problems within one area of the HAN system should not impact other areas of the HAN system*
  - *Information crossing any boundary should be validated for reasonability, expected accuracy, and possible modification, with anomalies timestamped and logged, and/or alarmed.*

- Communication integrity *(DHS-CSC 2.8.8)*
  - *Integrity requirements for HAN devices can vary in importance*

  - *For information with high integrity requirements, authentication of the source of the information should be used. This authentication may or may not require encryption of the information.*
  - *All information transmitted across the HAN system should be validated to the appropriate level of accuracy, using reasonability and validity checking methods.*
  - *Given the untrusted nature of the HAN system, critical information should always have backup or redundant means of access, including alternate communication paths, alternate sources (e.g. secondary voltage sources), default settings, or methods for estimation.*

- Communication confidentiality *(DHS-CSC 2.8.9)*
  - *Although it might appear that a customer does not require their information to be protected for confidentiality within their own home, their HAN systems are very vulnerable to unauthorized access both from deliberate attacks and from inadvertent disclosures due to poor configuration management. Therefore, confidentiality of data must be protected to better ensure the customer's privacy needs are met.*
  - *For information with high confidentiality requirements, cryptographic mechanisms should be used, as defined in appropriate security standards*
  - *The HAN system should be designed to handle the additional compute and communication traffic requirements to utilize the recommended cryptographic technologies.*

- Trusted path (DHS-CSC 2.8.10)
  - *Although very desirable, trusted paths in HAN networks cannot be expected.*
  - *Since so many different stakeholders, devices, and applications utilize HAN systems which are generally managed by customers without security expertise, trusted paths are not generally possible for HAN devices. Therefore, alternate security methods must be established for sensitive functions, such as requiring VPNs, validating all information flows, intrusion detection, checking for confidentiality compromises, and using alternate sources of this data for reasonability checking.*

- Cryptographic key establishment and management *(DHS-CSC 2.8.11)*
  - *Cryptography used for sensitive information should use key establishment and management techniques appropriate to meters, field equipment, and bandwidth-limited communications, recognizing that direct access to certificates by field equipment is generally not feasible.*
  - *Since HAN devices could have access to external (or intra-HAN) certificate management, key management should be designed into all sensitive HAN devices.*

- Transmission of security parameters *(DHS-CSC 2.8.14)*
  - *Security standards for HAN systems, when these become available (some through the IEC), should be used to ensure the secure transmission of security parameters.*

- Security roles (DHS-CSC 2.8.19)

- *Customers may or may not be in charge of security for each type of device on their HANs. For instance, utilities may be in charge of sub-metering security, vendors may be in charge of security for their devices, and ESPs may be in charge of DER devices or other energy-related devices.*
- *Role-Based Access Control (RBAC) should be used to establish precisely which individuals and applications play which roles, and what access authority each role has with respect to information being monitored and controlled over the interface.*
- *Role access authorization should allow for access restrictions on individual data items, in addition to access authorization by equipment and/or by groups of data. Not all devices on the HAN will require access on a per-data-item basis, but this level of access should be expected as required by some devices, particularly DER equipment and private customer databases.*

- Message authenticity *(DHS-CSC 2.8.20)*
  - *Message authentication must be performed by all devices on HAN networks.*
  - *IEC 62351 security standards should be used to authenticate messages where IEC protocol standards (such as IEC 61850) are used.*

- Fail in known state *(DHS-CSC 2.8.24)*
  - *All equipment should revert to a previously-defined default condition upon loss of communications. This default condition should ensure minimal disruption to critical systems. This is particularly important for DER equipment and other devices that could adversely affect the customer and/or the power system.*
  - *All failed equipment should not affect other equipment or disrupt critical systems.*

- Confidentiality of information at rest *(DHS-CSC 2.8.28)*
  - *HAN devices can contain information that must remain confidential and/or private. These devices should use cryptographic techniques to ensure the confidentiality of this information.*

3.3.3.4 Incident Response (DHS-CSC 2.12)

- Continuity of operations plan *(DHS-CSC 2.12.2)*
  - *Devices on HAN networks may or may not be involved in operations, such as response to Demand Response signals or direct control commands. However, if they are, automated plans should be in place for default or backup actions if an incident (deliberate attack or inadvertent mistake or equipment failure) prevents normal activities.*
  - *In particular, all DER equipment (and loads under load management) should have default settings or modes in case of the loss of communications beyond expected limits.*
  - *Critical information should be available from multiple sources if possible. If these additional sources have the information, but do not normally provide this*

information, then the incident plan should include methods for rapid access to these other sources.

- Continuity of operations roles and responsibilities *(DHS-CSC 2.12.3)*
  - *Energy service providers or other managers of DER devices and/or load control capabilities should have well defined roles in cases of loss of communications with the DER devices or loads.*
  - *Certain software applications and systems (such as tamper detection, revenue protection, confidentiality monitoring, and other tools) should be included the incident plan for monitoring, assessing, and controlling equipment during emergency situations.*

- Incident response training, testing, and update *(DHS-CSC 2.12.4, .5, .6)*
  - *As increased amounts of generation and storage are located at customer sites, power system training simulators and testing tools can help train utility and ESP personnel in handling security-related incidents.*
  - *Incident plans that are only on paper are virtually useless. Periodic training and testing must also take place, such as testing DER responses to different types of incidents, while not disrupting normal power system operations or compromising metering confidentiality.*

- Incident handling *(DHS-CSC 2.12.7)*
  - *Unlike some other systems, control systems cannot just be shut down during an incident – they must be kept running. Particularly critical is the response of DER devices at customer sites – should they turn off or keep operating? Significant additional work and standards are needed to manage these types of incidents.*
  - *HAN systems with customer-based DER devices should be designed to expect equipment and system failures, so that critical DER equipment can continue to perform as needed to help maintain power system reliability.*
  - *During an incident, the key will be to utilize the incident plans, but also be flexible and aware enough to respond to unexpected or unplanned for situations. This will take training, access to information from multiple sources, and the ability to try innovative approaches if the planned approach is not succeeding.*

- Incident monitoring *(DHS-CSC 2.12.8)*
  - *All anomalies should be monitored and assessed, both automatically, and if warranted, brought to the attention of a security operator. Sometimes what appears to be innocuous to a power system operator or an ESP management system could be a critical signal of a possible security attack to a security operator*
  - *Alarm and event monitoring of systems and equipment connected to the HAN system should include not only equipment and power system events, but also security events. This A&E monitoring could be an expansion of HAN system management.*
  - *All alarm and events should be assessed for security-related concerns as well as power system operational concerns or customer-related concerns.*

  - *Alarm and event logs should contain a synchronized timestamp that is appropriately accurate so that correlations across wide spread systems can take place*
  - *Disturbance analysis should be used for some types of critical situations, in which the state and measurements of the power system and/or the information system are captured and saved periodically (every 2-10 seconds for critical power system states), then discarded after a while if no incident occurs. If an incident does occur, then the sequence of periodic saved information can be critical to understanding what happened and how best to respond to it.*

- Incident reporting *(DHS-CSC 2.12.8)*
  - *All assessments of anomalies and/or alarms and events should be reported to the appropriate level so that any necessary correlations and corrective actions can take place*
  - *Often incidents are not reported outside a small group to avoid either embarrassment or the possibility that a different attacker would learn about it and use it again. However, great care should be taken not to use the latter excuse when the real reason is the former, since corrective action by other groups with similar vulnerabilities should also take place.*

- Control system backup *(DHS-CSC 2.12.16)*
  - *All critical HAN system data should be backed up, using standard methods for ensuring that bad data is not written over the good data*

- Control system recovery and reconstitution *(DHS-CSC 2.12.17)*
  - *All HAN systems should be designed so that authorized personnel can recover the previous state of the system after a deliberate attack or an inadvertent failure or mistake.*

3.3.3.5 System and Information Integrity (DHS-CSC 2.14)

- System monitoring tools and techniques *(DHS-CSC 2.14.4)*
  - *HAN networks, even the simplest home WiFi systems, should include intrusion detection for all components*
  - *Intrusions should be reported using the HAN system monitoring capabilities to identify and alarm security events.*
  - *If ESPs, vendors, and other external entities are responsible for security of specific devices within the HAN, they should also be notified.*

- Security alerts and advisories *(DHS-CSC 2.14.5)*
  - *HAN system alarm and event handling of events should be extended to security alarm and events of information system events, with such alarms being directed to security personnel.*

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

- *Communication protocols used over the HAN system should include authentication and integrity validation capabilities which may be used by devices as necessary.*
- *Devices on HAN systems should assess the validity of information received from the field equipment through multiple methods, such as reasonability assessment, redundancy, power flow-based estimations, etc.*
- *DER controllers on HAN systems that manage DER equipment should also monitor software changes, software halting, software restarts, etc.*
- *Availability of time-sensitive information should be monitored and alarmed if not available within the required timeframe. This availability should include DER information, software application execution results, and customer inputs.*

- Information input restrictions *(DHS-CSC 2.14.9)*
  - *RBAC should be implemented for all sensitive HAN devices to restrict input to authorized personnel and software applications.*

- Information input accuracy, completeness, validity, and authenticity *(DHS-CSC 2.14.10)*
  - *All input, whether from authorized personnel or software applications or inputs from sensors, should be checked as much as feasible for accuracy, completeness, validity, and authenticity.*
  - *All input to sensitive HAN devices should be validated as reasonable and within expected limits. Additional interactions should be used to validate unexpected inputs to ensure their authenticity and to ensure they are not mistakes.*

- Error handling (DHS-CSC 2.14.11)
  - *All errors, whether associated with inputs, software applications, communication errors, and/or sensor inputs, should be logged and the appropriate personnel notified.*
  - *Categorization and prioritization of errors should be provided to ensure the most important errors and alarms are sent to the appropriate personnel in a timely manner.*

3.3.3.6 Access Control (DHS-CSC 2.15)

- Access enforcement *(DHS-CSC 2.15.7)*
  - *Role-Based Access Control (RBAC) should be implemented for all HAN devices.*
  - *Role access authorization should allow for access restrictions on individual data items, in addition to access authorization by equipment and/or by groups of data. Not all devices on the HAN will require access on a per-data-item basis, but this level of access should be expected as required by some devices, particularly DER equipment and private customer databases.*
  - *If legacy equipment and communication constraints do not permit this level of access control, then compensating security methods should be provided, such as limiting access within the AMI system database.*

- Least privilege *(DHS-CSC 2.15.9)*
  - *Role-Based Access Control should use the concept of least privilege when designing roles and assigning individuals and applications to those roles. This is particularly important for sensitive information from HAN devices.*

- Permitted actions without identification or authentication *(DHS-CSC 2.15.11)*
  - *Monitoring and logging of ALL demand response and other control commands should be implemented, even during emergency overrides. Therefore, at least identification and logging of actions should be required.*

- Passwords (DHS-CSC 2.15.16)
  - *Passwords, using strong authentication, should be required for access to all HAN devices, and should be used in conjunction with RBAC.*
  - *Default passwords should be changed immediately upon installation of systems and equipment.*

- Wireless access restrictions *(DHS-CSC 2.15.26)*
  - *In the HAN environment both wired and wireless media are expected to be used for both economic and convenience reasons. No specific restrictions are foreseen, although the specific vulnerabilities of each should be taken into account.*
  - *Wireless systems have particular security vulnerabilities so that very clear guidelines should be developed to identify the security measures to be implemented and the types of information that are permitted and not permitted to go over wireless media. For instance, PEV chargers may restrict communications to wired media through the charging plug to ensure that the charging plug is actually connected to the PEV which has been authenticated.*
  - *Wired communications media have other types of security vulnerabilities, such as the ability to cut the media, thus providing a simple way for denial of service attacks.*

3.3.3.7 Audit and Accountability (DHS-CSC 2.16)

- Auditable events *(DHS-CSC 2.16.2)*
  - *All devices and systems on HANs should include logging capabilities.*
  - *Power system events, customer-based events, and all security-related events should be logged and timestamped for later analysis.*
  - *Categories and priorities of events should be established to ensure critical event information is provided to the right person or application for responding in a timely manner.*

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

– *Time synchronization should be provided for all HAN-based devices.*

3.4 Interface Category 12: Interfaces between External Systems and the Customer Site

Interface Category 12 is focused on the interfaces between external systems and the customer site through the Energy Services Interface (ESI) or HAN Gateway. *(This category excludes the interfaces used for direct DER and load control which is covered by Interface Category 1b, and the AMI system interface which is covered by Interface Category 10*).

One primary type of security requirements is paramount in Interface Category 12 – Interfaces between external parties and the customer site:

- **Customer and application confidentiality and/or privacy, since so many stakeholders have some degree of access across the ESI/HAN Gateway. This stakeholder access must be well managed.**

Clearly integrity and availability can be important for individual functions across the ESI/HAN gateway, particularly those involving signaling for DER and load management, but the key general requirement is for confidentiality and/or privacy across this very public interface.

Interactions via Interface Category 12 could use either public networks (e.g. the public Internet, cable network, or the cellphone GPRS system) or private networks (e.g. DER or load management networks provided by ESPs). All of these interfaces are required to go through a "HAN gateway" or an Energy Services Interface (ESI), although the nature and configuration of such gateways are not specified. This HAN gateway could be distributed, such that it is included within different devices, and/or it could be a single entry point to the customer site. The key requirement is that there is some "black box" that acts as protection, isolating the HAN devices from direct access by external parties.

Private networks would probably be used more for specific functions, such as DER and load management by energy service providers, and would most likely interface directly with "HAN Gateways" at the appropriate controllers and devices at the customer site. However, some private networks could also interface with the customer's network through an ESI or other gateway. Unlike the tightly-coupled control commands covered in Interface Category 1b interactions, these Interfaced Category 12 interactions would be "loosely coupled", with the ESP providing signals that could be interpreted by the local DER and load controllers and used in their management strategies.

The majority of stakeholders (vendors, maintenance providers, general energy service providers) would most likely use the existing public networks to connect to a HAN or similar customer-site network.

Although private networks might appear to be more secure since they entail normal access by fewer stakeholders, they could be actually be less secure if the external party and/or HAN system does not provide adequate security.

Both wired and wireless technologies would be used in these public/private networks. Since the interactions are expected to be "loosely-coupled", availability is not a high concern so neither of these technologies would pose any particular problem if appropriately secured.

Although there could be some security key management issues, solutions can probably be found in the IT community, unlike the Interface Categories 1a – 1d, and 10 which will require special key management techniques.

These interfaces include those:

- Between ESPs and HAN Gateways
- Between Third Party vendors and HAN Gateway
- Between any non-metering entity and the Energy Services Interface (ESI) / HAN Gateway

3.4.1 Interface Category 12 Characteristics

The following are the key characteristics of Interface Category 12, although clearly some interactions will have only some of these characteristics, while others will have some of the other characteristics.

- Cst-1a: High requirement for confidentiality which necessitates or strongly influences the types of security measures required.
- Cst-1b: High requirement for privacy which necessitates or strongly influences the types of security measures required.
- Cst-5: *Microprocessor constraints on memory and compute capabilities* which limits the types of security measures which could be employed.
- Cst-7: *Immature or proprietary protocols* which may not be adequately tested either against inadvertent compromises or deliberate attacks.
- Cst-8: *Cross-organizational interactions* which limit trust and compatibility of security policies and measures, including the use of out-sourced services and leased networks.
- Cst-12: *Insecure locations* which cannot be made more secure due to their physical environment or ownership.
- Cst-15: *Unknown or rapidly changing types of interactions* which complicate the decisions on the types and severity of security threats and impacts.
- Cst-16: *Environmental and physical access constraints* which limit the types of security measures, particularly physical security.
- Cst-22: *Novel business functions with unknown ramifications from security breaches* which can either lead to unwarranted, burdensome security measures or, more likely, inadequate security measures.

3.4.2 Specific Interface Category 12 Security-Related Issues

The security-related issues for this external interface to the customer site include the following:

- Some information exchanged among different appliances and systems must be treated as confidential and private to ensure that an unauthorized third party does not gain access to it. For instance, energy usage statistics from the customer site that are sent through the ESI/HAN gateway must be kept confidential from other appliances whose vendors may want to scavenge this information for marketing purposes.
- Integrity of data is clearly important in general, but since so many different types of interactions are taking place, the integrity requirements will need to be specific to the particular application.
- Availability is generally not very critical between external parties and the customer site since most interactions are not related to power system operations nor are they needed in real-time. Even DER generation and storage devices have their own integrated controllers which are normally expected to run independently of any direct monitoring and control, and should have "default" modes of operation to avoid any power system problems.
- Bandwidth is not generally a concern, since higher speed media can be used if a function requires higher volume of data traffic. Many different types of media, particularly public media, is increasingly available, including the public Internet over cable or DSL, campus or corporate Intranets, cellphone GPRS, and neighborhood WiMax and WiFi systems.
- Some customer devices that contain their own "HAN gateway" firewall are constrained in their compute capabilities, primarily to keep costs down, which may limit the types and layers of security which could be applied with those devices.
- Other than those used over the public Internet, communication protocols between Third Parties and ESI/HAN Gateways have not yet stabilized as accepted standards, nor have their capabilities been proven through rigorous testing.
- ESI/HAN Gateways will be accessible by many different vendors and organizations with unknown corporate security requirements and equally variable degrees and types of security solutions. Even if one particular interaction is "secure", in aggregate these multiplicity of interactions may not be secure.
- ESI/HAN Gateways may be in physically insecure locations, thus limiting physical security. Even those presumably "physically secure" within a home are vulnerable to inadvertent situations such as poor maintenance and mis-use, as well as break-ins and theft.
- Many possible future interactions within the HAN environment are still being designed, or are just being speculated about, or have not yet been conceived, leading to many possible but unknown security issues.

3.4.3 Security Control Requirements for Interface Category 12

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

3.4.3.1 Physical and Environmental Security (DHS-CSC 2.4)

- Physical access control *(DHS-CSC 2.4.3)*
  - *ESI/HAN Gateways will be physically insecure so alternate security means should be implemented, such as logging all power on/off events and requiring very strong cryptographic technologies for all interactions so that theft would not compromise customer information.*

- Monitoring physical access *(DHS-CSC 2.4.4)*
  - *Given the vulnerability of ESI/HAN Gateways to physical access, they should, at a minimum, self-monitor for inappropriate physical access, and when possible, log the event and take other appropriate action such as shutting off.*
  - *External network connections and HAN network connections to ESI/HAN Gateways should also be monitored and logged for physical access, such as unplugging connectors or restarting components.*

3.4.3.2 Configuration Management (DHS-CSC 2.6)

- Configuration change control *(DHS-CSC 2.6.3)*
  - *ESI/HAN Gateways configuration management is critical for ensuring appropriate confidentiality and privacy. The most likely configuration changes will occur when new HAN devices are added or moved that the ESI/HAN Gateways must "register" and/or learn their HAN address. Although ultimately the HAN configuration is the responsibility of the customer, all HAN devices and HAN communication nodes should include testing of configuration changes for validity and unintended consequences, and the ability to "roll-back" or "undo" any changes that do not meet the permissibility, availability and/or other requirements.*

- Monitoring configuration changes *(DHS-CSC 2.6.4)*
  - *ESI/HAN Gateway configurations can be physically changed and/or logically changed. Both types of changes should be monitored.*
  - *Monitoring configuration changes for ESI/HAN Gateways should ensure that all authorized "stakeholders" receive (or are permitted to receive) notification of changes that impact them.*

- Access restrictions for configuration changes *(DHS-CSC 2.6.5)*
  - *RBAC should be used to restrict access to making configuration changes to the ESI/HAN Gateway to authorized personnel (e.g. customer) and software applications.*

- Configuration settings *(DHS-CSC 2.6.6)*

- *RBAC should be used to restrict access to making changes to settings and parameters of the ESI/HAN Gateway to authorized personnel (e.g. customer) and software applications.*

- Factory default authentication management *(DHS-CSC 2.6.10)*
  - *ESI/HAN Gateways should have factory-provided default certificates to secure them from tampering, from the addition of Trojan horses, or from other security breaches during shipment. These certificates should be changed when installed in the field.*

3.4.3.3 System and Communication Protection (DHS-CSC 2.8)

- Security function isolation *(DHS-CSC 2.8.3)*
  - *The ESI/HAN Gateway provides many of the security functions. If its security functions are managed by an external party, then these interactions should be strongly protected, but may not necessarily be isolated from other interactions.*
  - *Many "security functions" are actually part of the normal HAN network and system management in which HAN nodes, communications, and end devices are monitored for anomalous events, and actions taken to mitigate problems, whether deliberately or inadvertently caused. Therefore, these security functions should not be isolated from normal operations.*
  - *Some security functions, such as establishing access controls, key management, and information prioritization and flow control, should be separated from operational functions.*

- Denial of service protection *(DHS-CSC 2.8.5)*
  - *Although availability security requirements are not generally very stringent for ESI/HAN Gateways, for circumstances where availability is critical, certain protection such as redundancy, backup, alternate sources of power, alternate sources of data, etc., could be used.*
  - *Network and System Management (NSM) should provide intrusion detection and resource exhaustion detection, with notification of these events securely provided to appropriate personnel and/or systems.*
  - *ESI/HAN Gateways should use SNMP and other NSM technologies to help monitor and/or manage the HAN networks such as providing communication path monitoring to detect permanent and temporary path failures, as well as equipment and software failures*

- Resource priority *(DHS-CSC 2.8.6)*
  - *Priority of different types of data should be clearly defined and implemented for ESI/HAN Gateways.*
  - *For similar time latency requirements, higher priority data should be retrieved before lower priority data.*
  - *During emergencies, priority of data should be strictly enforced, including the rejection of all low priority data.*

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

- Boundary protection *(DHS-CSC 2.8.7)*
  - *ESI/HAN Gateways provide boundary protection between external systems and HAN-based devices and systems, and should also manage the boundaries between multi-network HANs. For multi-network HAN systems, boundaries should be clearly defined, including at least separate boundaries for any sub-metering information, for devices requiring tightly-coupled management (e.g. DER control), for devices needing only loosely-coupled interactions (e.g. HVAC), for security management information, for sensitive customer information, and for "public" information*
  - *These HAN system boundaries should be protected as appropriate and as feasible through physical separation, virtual separation, layered security, RBAC, and/or other security mechanisms.*
  - *Information traffic across these boundaries should be avoided, or, if necessary, secured through the ESI/HAN Gateway or similar functionality.*
  - *Any cross-boundary interactions should be monitored and logged, with unexpected interactions causing alarms*
  - *Access to data transmitted across the HAN system boundaries should be limited to authorized systems through RBAC procedures as much as feasible.*
  - *Security problems within one area of the HAN system should not impact other areas of the HAN system*
  - *Information crossing any boundary should be validated for reasonability, expected accuracy, and possible modification, with anomalies timestamped and logged, and/or alarmed.*

- Communication integrity *(DHS-CSC 2.8.8)*
  - *Integrity requirements for HAN devices can vary in importance. For information with high integrity requirements, the ESI/HAN Gateway should authenticate the source of the information. This authentication may or may not require encryption of the information.*
  - *All information transmitted from external systems through the ESI/HAN Gateway should be validated to the appropriate level of accuracy, using reasonability and validity checking methods. The same requirement should apply to HAN devices transmitting information to external systems.*
  - *Given the untrusted nature of the HAN system, critical information should always have backup or redundant means of access, including alternate communication paths, alternate sources (e.g. secondary voltage sources), default settings, or methods for estimation.*

- Communication confidentiality *(DHS-CSC 2.8.9)*
  - *The ESI/HAN Gateway must ensure the confidentiality of HAN data being transmitted through it to external systems to better ensure the customer's privacy needs are met.*

  - *The ESI/HAN Gateway should use strong cryptographic mechanisms, as defined in appropriate security standards*
  - *The ESI/HAN Gateway should be designed to handle the additional compute and communication traffic requirements to utilize the recommended cryptographic technologies.*

- Trusted path (DHS-CSC 2.8.10)
  - *Since so many different stakeholders will be exchanging information through the ESI/HAN Gateway to interact with HAN devices and applications which are generally managed by customers without security expertise, trusted paths are not generally possible for HAN devices. Therefore, alternate security methods must be established for sensitive functions, such as requiring VPNs, validating all information flows, intrusion detection, checking for confidentiality compromises, and using alternate sources of this data for reasonability checking.*

- Cryptographic key establishment and management *(DHS-CSC 2.8.11)*
  - *Cryptography used for sensitive information should use key establishment and management techniques appropriate to meters, field equipment, and bandwidth-limited communications, recognizing that direct access to certificates by field equipment is generally not feasible.*
  - *Since the ESI/HAN Gateway will act as at least one route for HAN devices to access external certificate management, it should be able to securely manage such key management..*

- Transmission of security parameters *(DHS-CSC 2.8.14)*
  - *Security standards for HAN systems, when these become available (some through the IEC), should be used to ensure the secure transmission of security parameters.*

- Security roles (DHS-CSC 2.8.19)
  - *ESI/HAN Gateways should support the security roles established for the HAN. For instance, customers may or may not be in charge of security for each type of device on their HANs. For instance, utilities may be in charge of sub-metering security, vendors may be in charge of security for their devices, and ESPs may be in charge of DER devices or other energy-related devices.*
  - *Role-Based Access Control (RBAC) should be used to establish precisely which individuals and applications play which roles, and what access authority each role has with respect to information being monitored and controlled over the interface.*
  - *Role access authorization should allow for access restrictions on individual data items, in addition to access authorization by equipment and/or by groups of data. Not all devices on the HAN will require access on a per-data-item basis, but this level of access should be expected as required by some devices, particularly DER equipment and private customer databases.*

- Message authenticity *(DHS-CSC 2.8.20)*

  - *The ESI/HAN Gateway should perform message authentication for all devices on HAN networks.*
  - *IEC 62351 security standards should be used to authenticate messages where IEC protocol standards (such as IEC 61850) are used.*

- Fail in known state *(DHS-CSC 2.8.24)*
  - *All equipment should revert to a previously-defined default condition upon loss of communications. This default condition should ensure minimal disruption to critical systems. This is particularly important for DER equipment and other devices that could adversely affect the customer and/or the power system.*
  - *All failed equipment should not affect other equipment or disrupt critical systems.*

- Confidentiality of information at rest *(DHS-CSC 2.8.28)*
  - *ESI/HAN Gateways can contain information that must remain confidential and/or private. They should use cryptographic techniques to ensure the confidentiality of this information.*

3.4.3.4 Incident Response (DHS-CSC 2.12)

- Continuity of operations plan *(DHS-CSC 2.12.2)*
  - *Devices on HAN networks may or may not be involved in operations, such as response to Demand Response signals or direct control commands. However, if they are, automated plans should be in place for default or backup actions if an incident affecting the ESI/HAN Gateway (deliberate attack or inadvertent mistake or equipment failure) prevents normal activities.*
  - *In particular, all DER equipment (and loads under load management) should have default settings or modes in case of the loss of communications beyond expected limits.*
  - *Critical information should be available from multiple sources if possible. If these additional sources have the information, but do not normally provide this information, then the incident plan should include methods for rapid access to these other sources.*

- Continuity of operations roles and responsibilities *(DHS-CSC 2.12.3)*
  - *Energy service providers or other managers of DER devices and/or load control capabilities should have well defined roles in cases of loss of communications through the ESI/HAN Gateway with the DER devices or loads.*
  - *Certain software applications and systems (such as tamper detection, revenue protection, confidentiality monitoring, and other tools) should be included the incident plan for monitoring, assessing, and controlling equipment during emergency situations.*

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

- *As increased amounts of generation and storage are located at customer sites, power system training simulators and testing tools can help train utility and ESP personnel in handling security-related incidents.*
- *Incident plans that are only on paper are virtually useless. Periodic training and testing must also take place, such as testing DER responses to different types of incidents, while not disrupting normal power system operations or compromising metering confidentiality.*

- Incident handling *(DHS-CSC 2.12.7)*
  - *Unlike some other systems, control systems cannot just be shut down during an incident – they must be kept running. Particularly critical is the response of DER devices at customer sites – should they turn off or keep operating? Significant additional work and standards are needed to manage these types of incidents.*
  - *ESI/HAN Gateways that interact with customer-based DER devices should be designed to expect equipment and system failures, so that critical DER equipment can continue to perform as needed to help maintain power system reliability.*
  - *During an incident, the key will be to utilize the incident plans, but also be flexible and aware enough to respond to unexpected or unplanned for situations. This will take training, access to information from multiple sources, and the ability to try innovative approaches if the planned approach is not succeeding.*

- Incident monitoring *(DHS-CSC 2.12.8)*
  - *All anomalies should be monitored and assessed, both automatically, and if warranted, brought to the attention of a security operator. Sometimes what appears to be innocuous to a power system operator or an ESP management system could be a critical signal of a possible security attack to a security operator*
  - *Alarm and event monitoring of systems and equipment connected to the ESI/HAN Gateway should include not only equipment and power system events, but also security events.*
  - *All alarm and events should be assessed for security-related concerns as well as power system operational concerns or customer-related concerns.*
  - *Alarm and event logs on ESI/HAN Gateways should contain a synchronized timestamp that is appropriately accurate so that correlations across wide spread systems can take place.*
  - *Disturbance analysis should be used for some types of critical situations, in which the state and measurements of the power system and/or the information system are captured and saved periodically (every 2-10 seconds for critical power system states), then discarded after a while if no incident occurs. If an incident does occur, then the sequence of periodic saved information can be critical to understanding what happened and how best to respond to it.*

- Incident reporting *(DHS-CSC 2.12.8)*

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

- Control system backup *(DHS-CSC 2.12.16)*
  - *All critical ESI/HAN Gateway data should be backed up, using standard methods for ensuring that bad data is not written over the good data*

- Control system recovery and reconstitution *(DHS-CSC 2.12.17)*
  - *All ESI/HAN Gateway should be designed so that authorized personnel can recover the previous state of the system after a deliberate attack or an inadvertent failure or mistake.*

3.4.3.5 System and Information Integrity (DHS-CSC 2.14)

- System monitoring tools and techniques *(DHS-CSC 2.14.4)*
  - *ESI/HAN Gateways should include intrusion detection for all components*
  - *Intrusions should be reported using the HAN system monitoring capabilities to identify and alarm security events.*
  - *If ESPs, vendors, and other external entities are responsible for security of specific devices within the HAN, the ESI/HAN Gateway should notify them.*

- Security alerts and advisories *(DHS-CSC 2.14.5)*
  - *ESI/HAN Gateway alarm and event handling of events should be extended to security alarm and events of information system events, with such alarms being directed to security personnel.*

- Software and information integrity *(DHS-CSC 2.14.7)*
  - *Communication protocols used with the ESI/HAN Gateway should include authentication and integrity validation capabilities which may be used by devices as necessary.*
  - *Devices on HAN systems should assess the validity of information received from the field equipment through multiple methods, such as reasonability assessment, redundancy, power flow-based estimations, etc.*
  - *DER controllers on HAN systems that manage DER equipment should also monitor software changes, software halting, software restarts, etc.*
  - *Availability of time-sensitive information should be monitored and alarmed if not available within the required timeframe. This availability should include DER information, software application execution results, and customer inputs.*

- Information input restrictions *(DHS-CSC 2.14.9)*
  - *RBAC should be implemented with the ESI/HAN Gateway for all sensitive HAN devices to restrict input to authorized personnel and software applications.*

- Information input accuracy, completeness, validity, and authenticity *(DHS-CSC 2.14.10)*
  - *All input, whether from authorized personnel or software applications or inputs from sensors, should be checked as much as feasible for accuracy, completeness, validity, and authenticity.*
  - *All input to ESI/HAN Gateways should be validated as reasonable and within expected limits. Additional interactions should be used to validate unexpected inputs to ensure their authenticity and to ensure they are not mistakes.*

- Error handling (DHS-CSC 2.14.11)
  - *All errors, whether associated with inputs, software applications, communication errors, and/or sensor inputs, should be logged and the appropriate personnel notified.*
  - *Categorization and prioritization of errors should be provided to ensure the most important errors and alarms are sent to the appropriate personnel in a timely manner.*

3.4.3.6 Access Control (DHS-CSC 2.15)

- Access enforcement *(DHS-CSC 2.15.7)*
  - *The ESI/HAN Gateway should enforce access control between external systems and all HAN-based systems.*
  - *Role-Based Access Control (RBAC) should be implemented for all HAN devices.*
  - *Role access authorization should allow for access restrictions on individual data items, in addition to access authorization by equipment and/or by groups of data. Not all devices on the HAN will require access on a per-data-item basis, but this level of access should be expected as required by some devices, particularly DER equipment and private customer databases.*
  - *If legacy equipment and communication constraints do not permit this level of access control, then compensating security methods should be provided, such as limiting access within the AMI system database.*

- Least privilege *(DHS-CSC 2.15.9)*
  - *Role-Based Access Control should use the concept of least privilege when designing roles and assigning individuals and applications to those roles. This is particularly important for sensitive information from HAN devices.*

- Permitted actions without identification or authentication *(DHS-CSC 2.15.11)*
  - *Monitoring and logging of ALL demand response and other control commands should be implemented, even during emergency overrides. Therefore, at least identification and logging of actions should be required.*

- Passwords (DHS-CSC 2.15.16)
  - *Passwords, using strong authentication, should be required for access to all HAN devices, and should be used in conjunction with RBAC.*
  - *Default passwords should be changed immediately upon installation of systems and equipment.*

3.4.3.7 Audit and Accountability (DHS-CSC 2.16)

- Auditable events *(DHS-CSC 2.16.2)*
  - *All devices and systems on HANs should include logging capabilities.*
  - *Power system events, customer-based events, and all security-related events should be logged and timestamped for later analysis.*
  - *Categories and priorities of events should be established to ensure critical event information is provided to the right person or application for responding in a timely manner.*

- Time stamps (DHS-CSC 2.16.8)
  - *ESI/HAN Gateways should be time-synchronized with NIST time. It should be able to provide time synchronization to all HAN-based devices that cannot otherwise be time synchronized.*
  - *Appropriately accurate timestamps are critical to being able to reconstruct the sequence of events, particularly across different systems and regions. Therefore timestamp accuracy and granularity should be determined for different types of events and/or equipment.*

3.5 Interface Category 14: Metering Interfaces

The main metering interactions in the HAN are those between devices and their sub-meters, as well as between those sub-meters and the primary customer meter.

3.5.1 Interface Category 14 Characteristics

- Cst-1: High requirement for confidentiality and/or privacy which necessitates or strongly influences the types of security measures required.
- Cst-2: High requirement for integrity and/or accuracy of data which influences not only the types of typical security measures, but also necessitates strong accuracy and error checking.
- Cst-4: *Low bandwidth of communications channels* which limits the types of security measures which could be employed per channel.

- Cst-5: *Microprocessor constraints on memory and compute capabilities* which limits the types of security measures which could be employed.
- Cst-6: *Wireless media* which can pose certain types of additional security challenges.
- Cst-7: *Immature or proprietary protocols* which may not be adequately tested either against inadvertent compromises or deliberate attacks.
- Cst-8: *Cross-organizational interactions* which limit trust and compatibility of security policies and measures, including the use of out-sourced services and leased networks.
- Cst-10: *Legacy end-devices and systems* which limit the types, thoroughness, or effectiveness of different security measures which could be employed.
- Cst-11: *Legacy communication protocols* which limit the types, thoroughness, or effectiveness of different security measures which could be employed.
- Cst-12: *Insecure locations* which cannot be made more secure due to their physical environment or ownership.
- Cst-13: *Key management for large numbers of devices* which can limit the methods for deploying and revoking keys.
- Cst-14: *Patch and update management constraints for sensitive devices* which limits the frequency of updating security patches.
- Cst-16: *Environmental and physical access constraints* which limit the types of security measures, particularly physical security.

3.5.2 Specific Interface Category 14 Issues

The issues for this Metering Interface Category include the following:

- Most metering information from the customer must be treated as confidential since profiles of hourly energy usage (as opposed to monthly energy usage) could be used for unauthorized and/or illegal activities.
- Integrity of revenue-grade metering data is vital since it has a direct financial impact on all stakeholders of the loads and generation being metered.
- Availability of metering data is important but not critical, since alternate means for retrieving metering data can still be used.
- Meters are constrained in their compute capabilities, primarily to keep costs down, which may limit the types and layers of security which could be applied.
- Revenue-grade meters must be certified, so that patches and upgrades require extensive testing and validation
- Key management of millions of meters will pose significant challenges that have not yet been addressed as standards

- Due to the relatively new technologies used with smart meters, some standards have not been fully developed, nor have their capabilities been proven through rigorous testing.
- Multiple (authorized) stakeholders, including customers, utilities, and third parties, may need access to energy usage either directly from the meter or after it has been processed and validated for settlements and billing, thus adding cross-organizational security concerns.
- Utility-owned meters are in physically insecure locations that are not under utility control, limiting physical security
- Local laptops or maintenance tools are connected by field installers and maintenance crews to manage meters and certain HAN appliances.

Some examples include interfaces:

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

3.5.3 Security Control Requirements for Interface Category 14

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

3.5.3.1 Physical and Environmental Security (DHS-CSC 2.4)

- Physical access control *(DHS-CSC 2.4.3)*
  - *Since meters cannot prevent access by customers and other people, very strong cryptographic technologies should be implemented for registers, databases, and other sensitive material within the meter*
  - *In particular, cryptographic keys should be stored encrypted and non-contiguously, and should never be copied into RAM.*
- Monitoring physical access *(DHS-CSC 2.4.4)*
  - *Given the vulnerability of meters to physical access, monitoring physical access should be designed into the meter and any of its interfaces with metered equipment*
  - *Tamper detection has been a meter requirement for many years. Using this capability can also help monitor physical access.*

- *Locks, limited physical access, and physical protection should be used for the interface between the equipment being metered and the meter*

3.5.3.2 Configuration Management (DHS-CSC 2.6)

- Configuration change control *(DHS-CSC 2.6.3)*
  - *Configuration management of metering equipment is critical for ensuring high integrity, and therefore changes should be very carefully controlled, including authorization through RBAC, testing of configuration changes for validity and unintended consequences, and the ability to "roll-back" any changes that do not meet the availability and/or other requirements.*
  - *Configurations can be physically changed and/or logically changed. Both types of changes should be controlled.*
  - *Configurations can be changed temporarily to handle maintenance, repair, testing, etc. Configurations can also be changed permanently. Both types of configuration changes should be controlled.*
  - *All configuration changes should be timestamped and logged, with the entity making the changes identified, as well as the type of configuration changes clearly described*

- Monitoring configuration changes *(DHS-CSC 2.6.4)*
  - *Meters and sub-meters should be monitored for configuration changes.*
  - *In particular, the connection path between the meter and any sub-meters should be monitored so that any changes that are outside "normal" path, such as variations in any meshed portions of the network, can be alarmed.*
  - *Inability to access a meter or sub-meter previously accessible should be alarmed after a "reasonable" timeframe.*
  - *Monitoring configuration changes for systems not under the control of a single organization should ensure that all "stakeholders" receive (or are permitted to receive) notification of changes.*

- Access restrictions for configuration changes *(DHS-CSC 2.6.5)*
  - *RBAC should be used to restrict access to making configuration changes to the metering equipment to authorized personnel and software applications*

- Configuration settings *(DHS-CSC 2.6.6)*
  - *RBAC should be used to restrict access to making changes to settings and parameters of the metering equipment to authorized personnel and software applications*

- Configuration for least functionality *(DHS-CSC 2.6.7)*
  - *Metering equipment should be strictly limited to known metering functions*

- Factory default authentication management *(DHS-CSC 2.6.10)*
  - *Meters should have factory-provided default certificates to secure them during shipment. These certificates should be changed to utility-provided certificates upon*

arrival and warehousing. Another certificate change should occur when installed in the field.

3.5.3.3 System and Communication Protection (DHS-CSC 2.8)

- Security function isolation *(DHS-CSC 2.8.3)*
  - *Many "security functions" are actually part of the normal metering procedures where they are monitored for anomalous events, and actions taken to mitigate problems, whether deliberately or inadvertently caused. Therefore, these security functions should not be isolated from normal operations.*
  - *Some security functions, such as establishing access controls, key management, and information prioritization and flow control, should be separated from metrology functions.*

- Denial of service protection *(DHS-CSC 2.8.5)*
  - *For some metering, availability requirements are significant. In those cases, redundancy of equipment, alternate paths, battery backup, and other methods should be provided for improving availability.*
  - *For metering with less stringent availability requirements, alternate methods for retrieving metering information can be used, such as on-site meter reading, estimated readings, etc.*
  - *Network and System Management (NSM) should provide intrusion detection and resource exhaustion detection for metering systems, with notification of these events securely provided to appropriate personnel and/or systems.*
  - *Wireless media can be particularly vulnerable to denial of service attacks if not properly configured, so mechanisms should be provided to, at a minimum, detect denial of service, and, for time-critical data, to provide alternate means to acquire this data either through redundancy or estimation, as appropriate.*

- Resource priority *(DHS-CSC 2.8.6)*
  - *Priority of different types of metering data should be clearly defined and identified to systems requiring access to the data. This includes priority handling of outage detection, priority identification of metering data needed for critical distribution functions, and metering data for critical locations such as first responders.*
  - *For similar time latency requirements, higher priority data should be retrieved before lower priority data*
  - *During emergencies, priority of data retrieval should be strictly enforced, including the rejection of all low priority data*
  - *No critical metering data should be lost or overwritten due to communication failures or low priority, so that it can be retrieved at a later time with no loss of accuracy.*

- Boundary protection *(DHS-CSC 2.8.7)*

  - *Metering boundaries should be clearly defined, including separate boundaries for metrology information, for security management information, for sensitive customer information, and for non-utility "public" information.*
  - *These metering boundaries should be protected as appropriate and as feasible through physical separation, virtual separation, layered security, RBAC, and/or other security mechanisms.*
  - *Metering information crossing any boundary should be validated for reasonability, expected accuracy, and possible modification, with anomalies timestamped and logged, and/or alarmed.*
  - *Information traffic across these boundaries should be avoided*
  - *Any cross-boundary interactions should be monitored and logged, with unexpected interactions causing alarms*
  - *Security problems within another area of the AMI system should not impact metering equipment.*

- Communication integrity *(DHS-CSC 2.8.8)*
  - *Revenue metering information has high integrity requirements, so authentication of the meter should be used. This authentication may or may not require encryption of the information.*
  - *All metering information transmitted across an AMI system should be validated to the appropriate level of accuracy, using VEE practices where appropriate or other similar reasonability and validity checking methods.*
  - *Given the untrusted nature of the AMI system, critical metering information should always have backup or redundant means of access, including alternate communication paths (e.g. truck-roll), alternate sources (e.g. secondary voltage sources), or methods for estimation (e.g. VEE or State Estimation function).*

- Communication confidentiality *(DHS-CSC 2.8.9)*
  - *Most smart metering information should be considered confidential, since hourly energy usage information can be used for unauthorized or illegal activities, such as unauthorized targeting of customers for marketing purposes, or burglary if the customer site appears empty due to low energy usage.*
  - *For metering information with high confidentiality requirements, cryptographic mechanisms should be used.*
  - *The AMI system and its components should be designed to handle the additional compute and communication traffic requirements to utilize the recommended cryptographic technologies.*

- Trusted path (DHS-CSC 2.8.10)
  - *Since metering equipment is located at untrusted sites, no completely trusted paths exist even between meters and sub-meters. Therefore, all metering information should be validated and checked for confidentiality compromises, and certain sensitive data should checked periodically against alternate sources of this data.*

- Cryptographic key establishment and management *(DHS-CSC 2.8.11)*
  - *Cryptographic techniques used for sensitive metering information should use key establishment and management techniques appropriate to the constraints posed by millions of meters, meter compute-constraints, and bandwidth-limited communications, while recognizing that direct access to certificates by meters is generally not feasible.*
  - *Key management for large numbers of meters and bandwidth-limited communication channels has not been developed as yet. This effort is underway in the IEC 62351 standards, and should be implemented when finalized.*
  - *"Bump-in-the-wire" security technology should not be used with meters given the lack of trust between the meter and any external equipment*

- Transmission of security parameters *(DHS-CSC 2.8.14)*
  - *Security standards for meters, when available, should be used to ensure the secure transmission of security parameters. These could include the ANSI C12.22, and IEC standards*

- Security roles (DHS-CSC 2.8.19)
  - *Role-Based Access Control (RBAC) should be used to establish precisely which individuals and applications play which roles, and what access authority each role has with respect to information being monitored and controlled over the interface.*
  - *Role access authorization should be per data item, not just by equipment or group of data.*
  - *If legacy equipment and/or bandwidth-limited communication protocols do not permit per data item access control, then compensating security methods should be provided at the enterprise level to limit access to data items in databases.*

- Message authenticity *(DHS-CSC 2.8.20)*
  - *ANSI C12.22, IEC 62351, and/or other IEC security standards should be used to authenticate messages*

- Fail in known state *(DHS-CSC 2.8.24)*
  - *All failed metering equipment should not affect other equipment or disrupt critical systems.*

- Confidentiality of information at rest *(DHS-CSC 2.8.28)*
  - *Metering equipment contains information within the meter that must remain confidential and/or private. This equipment should use cryptographic techniques to ensure the confidentiality of this information, such as database encryption.*

3.5.3.4 Incident Response (DHS-CSC 2.12)

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

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

- Continuity of operations roles and responsibilities *(DHS-CSC 2.12.3)*
  - *Metering incident planning should include the clear definition of roles to be played by all involved personnel*
  - *Certain software applications and systems (such as tamper detection, revenue protection, confidentiality monitoring, and other tools) should be included the incident plan for monitoring, assessing, and controlling metering equipment during emergency situations.*

- Incident response training, testing, and update *(DHS-CSC 2.12.4, .5, .6)*
  - *Incident plans that are only on paper are virtually useless. Periodic training and testing must also take place on the interfaces and equipment associated with this Interface Category – while not compromising metering confidentiality.*
  - *Power system training simulators and testing tools could be expanded to use information from metering to help train personnel in handling security-related incidents.*

- Incident handling *(DHS-CSC 2.12.7)*
  - *Unlike some other systems, control systems cannot just be shut down during an incident – they must be kept running. Metering may play an increasingly large role during incidents as providing redundant sources of potentially critical information.*
  - *During an incident, the key will be to utilize the incident plans, but also be flexible and aware enough to respond to unexpected or unplanned for situations. This will take training, access to information from multiple sources, and the ability to try innovative approaches if the planned approach is not succeeding.*

- Incident monitoring *(DHS-CSC 2.12.8)*
  - *All anomalies should be monitored and assessed, both automatically, and if warranted, brought to the attention of a security operator. Sometimes what appears to be innocuous to a power system operator or customer representative could be a critical signal of a possible security attack to a security operator*
  - *Alarm and event monitoring of metering equipment should include not only metering alarms and events, but also security alarms and events. This A&E monitoring could be an expansion of AMI system metering management.*
  - *All alarm and events should be assessed for security-related concerns as well as power system operational concerns or customer-related concerns.*
  - *Alarm and event logs should contain a synchronized timestamp that is appropriately accurate so that correlations across wide spread systems can take place*
  - *For some types of critical situations, the state and measurements of the power system and/or the information system should be captured and saved periodically (every 2-10 seconds for critical power system states), then discarded after a while if no incident*

occurs. If an incident does occur, then the sequence of periodic saved information can be critical to understanding what happened.

- Incident reporting *(DHS-CSC 2.12.8)*
  - *All assessments of metering anomalies and/or alarms and events should be reported to the appropriate level so that any necessary correlations and corrective actions can take place*
  - *Often incidents are not reported outside a small group to avoid either embarrassment or the possibility that a different attacker would learn about it and use it again. However, great care should be taken not to use the latter excuse when the real reason is the former, since corrective action by other groups with similar vulnerabilities should also take place.*

- Alternate control center *(DHS-CSC 2.12.15)*
  - *Alternate control centers may be needed by AMI systems as their functionality and criticality grow, including providing redundant operational data from metering equipment. The possibility for such an alternate center should be part of any design, even if not carried out in the near term.*

- Control system backup *(DHS-CSC 2.12.16)*
  - *All metering data should be backed up, using standard methods for ensuring that bad data is not written over the good data*

- Control system recovery and reconstitution *(DHS-CSC 2.12.17)*
  - *All metering systems should be designed so that authorized personnel can recover the previous state of the system after a deliberate attack or an inadvertent failure or mistake. This may include retrieving metering and other information by personnel physically visiting customer sites as well as using backup data.*

3.5.3.5 System and Information Integrity (DHS-CSC 2.14)

- System monitoring tools and techniques *(DHS-CSC 2.14.4)*
  - *Metering equipment should include intrusion detection for all components. Intrusions should be reported using the AMI system monitoring capabilities to identify and alarm security events.*
  - *If communication and equipment constraints do not permit this level of event monitoring, then compensating security methods should be provided, such as additional monitoring of equipment status to detect shut-downs, restarts, and physical access.*

- Security alerts and advisories *(DHS-CSC 2.14.5)*
  - *Metering alarm and event handling of events should be extended to security alarm and events of information system events, with such alarms being directed to security personnel.*

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

  - *All metering software and data should include authentication and integrity validation.*
  - *The validity of metered data should be assessed through multiple methods, such as revenue protection schemes, reasonability assessment, redundancy, estimations, etc.*
  - *Metering equipment should also log and alarm all software changes, software halting, software restarts, etc.*
  - *Availability of important information should be monitored and alarmed if not available within the required timeframe. This availability should include metering measurements, software application execution results, and personnel inputs.*

- Information input restrictions *(DHS-CSC 2.14.9)*
  - *RBAC should be implemented to restrict input to authorized personnel and software applications.*
  - *All information received from field locations should be strictly limited to authorized personnel, potentially with two-step authentication for critical interactions.*

- Information input accuracy, completeness, validity, and authenticity *(DHS-CSC 2.14.10)*
  - *All input, whether from authorized personnel or software applications or inputs from field sensors, should be checked as much as feasible for accuracy, completeness, validity, and authenticity.*
  - *Software patches and upgrades should be validated very extensively before being implemented on revenue grade metering equipment.*

- Error handling (DHS-CSC 2.14.11)
  - *All errors, whether associated with personnel inputs, software applications, communication errors, and/or sensor inputs, should be logged and the appropriate personnel notified*
  - *Categorization and prioritization of errors should be provided to ensure the most important errors and alarms are sent to the appropriate personnel in a timely manner.*

3.5.3.6 Access Control (DHS-CSC 2.15)

- Access enforcement *(DHS-CSC 2.15.7)*
  - *Role-Based Access Control (RBAC) should be implemented per data item, not just by equipment or group of data.*
  - *If legacy equipment and communication constraints do not permit this level of access control, then compensating security methods should be provided, such as limiting access within the metering database.*

- Least privilege *(DHS-CSC 2.15.9)*

- *Role-Based Access Control should use the concept of least privilege when designing roles and assigning individuals and applications to those roles. This is particularly important for sensitive information from metering equipment.*

- Permitted actions without identification or authentication *(DHS-CSC 2.15.11)*
  - *Monitoring and logging of ALL control commands should be implemented, even during emergency overrides. Therefore, at least identification and logging of actions should be required.*

- Passwords (DHS-CSC 2.15.16)
  - *Passwords, using strong authentication, should be required for all access to metering equipment, and should be used in conjunction with RBAC.*
  - *Default passwords should be changed immediately upon installation of systems metering equipment.*

- Wireless access restrictions *(DHS-CSC 2.15.26)*
  - *Wireless systems have particular security vulnerabilities so that very clear guidelines should be developed to identify the security measures to be implemented and the types of information that are permitted and not permitted to go over wireless media.*

3.5.3.7 Audit and Accountability (DHS-CSC 2.16)

- Auditable events *(DHS-CSC 2.16.2)*
  - *Metrology events, power system events, customer-based events, and all security-related events should be logged and timestamped in the metering equipment for later analysis.*
  - *Categories and priorities of events should be established to ensure critical event information is provided to the right person or application for responding in a timely manner.*

- Time stamps (DHS-CSC 2.16.8)
  - *Appropriately accurate timestamps are critical to being able to reconstruct the sequence of events, so timestamp accuracy and granularity should be determined for metering equipment.*
  - Time synchronization should be provide for all field equipment.