Section 5- GRID SECURITY AND CYBER SECURITY STRATEGY

5 GRID SECURITY AND CYBER SECURITY STRATEGY

5.1 INTRODUCTION

SDG&E intends to build a Smart Grid that is not only reliable and safe, but also secure. SDG&E is not alone in this expectation. The State of California[28] and the Commission agree that security plays a vital role in the state's electric infrastructure by stating "there is an urgent need to ensure that the utilities have appropriate security programs in place for physical and cyber threats and/or attacks."[29] In addition, the Federal Government, through Title XIII of the Energy Independence and Security Act of 2007 states that "it is the policy of the United States to support the modernization of the Nation's electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure that can meet future demand growth and to achieve each of the following, which together characterize a Smart Grid..."[30] From standards bodies, such as NIST, to utilities, to consumer advocacy groups and private citizens, everyone agrees that for Smart Grid to be successful it must be secure from physical and cyber threats and must protect the privacy of consumer data collected by utilities.

SDG&E sees three important aspects to achieving a secure Smart Grid, including physical security, cyber security and customer privacy. First, **physical security**, which includes preventing or reducing the threat of energy and property theft, vandalism, trespassing, and bomb scares, is a key part of the business of operating a utility. However, physical security becomes even more complex in a Smart Grid where infrastructure components and personnel previously confined to data centers will necessarily migrate out into the field where monitoring is more difficult and physical security intrusions experience longer response times. Second, **cyber security** programs will be challenged by an increasing number of cyber assets dispersed over a broader geographic area, controlling

[28] California Public Utilities Code, section 8360(a).
[29] D.10-06-047 at p.58[29] D.10-06-047 at p.58
[30] From the Energy Independence and Security Act of 2007, Public Law 110-140

more parts of the grid, and communicating more data than ever before. These assets will require protections against unauthorized access and losses to information confidentiality, integrity and availability that are at least as strong as their counterparts in data centers. Finally, **customer privacy** is a critical aspect to building and operating a secure Smart Grid. Pervasive customer privacy will require a set of robust business rules as well as effective security controls.

Information assets in the field will be hardened against physical tampering, and the grid itself better able to defend against unauthorized access to its systems and networks. Neither a physical nor a cyber-threat can be allowed to significantly impact the Smart Grid despite attacking any one or multiple parts of it. As hybrid physical-cyber threats emerge, SDG&E will prepare by considering how physical and cyber security programs can and will work together to protect Smart Grid assets and information. Security and privacy will be mandatory requirements that are designed in from the beginning.

5.1.1 SECURITY VISION AND APPROACH

To support SDG&E's larger vision for Smart Grid, the company is further elevating the already important role security, both physical and cyber, will play in this new paradigm. In this security perspective, SDG&E envisions that in the face of more complex systems with exponentially more data and transactions, an increased number of participants (customers consuming and producing energy, service providers, aggregators, regulators, utilities, etc.) will continue to rely on the availability of the system; trust the integrity of the information produced by the system; and be confident that sensitive information is secure from unauthorized access or disclosure. SDG&E's Smart Grid will be resistant to physical and cyber security threats, as well as resilient to attack and natural disasters. It will align with industry standards and best practices. SDG&E's security policies and practices are built on a security program that uses risk management methodologies to maximize its security investments.

To realize this vision, security programs and infrastructure will make Smart Grid participants **aware** of the risks and potential consequences. The utility will have greater visibility into the system state, as well as events taking place on the system; customers will understand how to better protect their privacy; each stakeholder will have more information to help the utility reduce the overall risk of the Smart Grid with an emphasis on creating a culture of security[31]. Security management functions will **converge**, being centrally governed by the utility. This management will allow for company-to-third-party interoperability. Company security processes, such as incident response, will be integrated. For system resistance and resilience, centrally managed security policies will **disaggregate**, distributing into localized islands or communities of infrastructure to allow the system to continue to protect itself in the event it becomes isolated from the total system environment. Finally, SDG&E will continue to focus and enhance its ability to **comply** with Federal, state and local regulations designed to protect the confidentiality, integrity and availability of the Smart Grid. SDG&E risk management methodologies will integrate with business processes and should eventually inform the development of mandatory reliability standards set by regulators. Over time, reliability standards should develop to align with the similar risk management frameworks in order to be agile, effective, and cost efficient.

This vision and approach will benefit all Smart Grid participants by allowing them to be confident that the system is reliable and dependable, its operation predictable and trustworthy, and free from unauthorized information disclosure or modification.

5.2 SECURITY RISKS IN THE SMART GRID

SDG&E evaluates three factors to measure a given risk to the Smart Grid: 1) threats to the system; 2) vulnerabilities in the system, and 3) the impact, or loss, if a threat successfully exploits vulnerability.

[31] Aligns with the Energy Sector Control System Working Group's "Roadmap to Secure Energy Delivery Systems."

Simply stated, **threats** are anything with the potential to cause harm. Lack of intent does not discount something as a threat. SDG&E classifies threats into three categories: Intentional, Accidental, and Environmental.

Intentional threats are those in which there is intent to adversely impact the confidentiality, integrity or availability of an asset. Common examples include sabotage, theft, cyber-attack, and malicious code (malware). In this category of threats, in the their report, *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System*, the North American Electric Reliability Corporation (NERC) and the Department of Energy (DOE) noted that "on the high-impact end of the scale are highly-coordinated, well-planned attacks against multiple assets designed to disable the system."[32] Intentional threats include not only these external sources, but insider threats such as disgruntled employees or contractors whose knowledge of the system and its vulnerabilities could be used to cause great harm.

Accidental threats include those human-caused events that may adversely impact an asset but in which there was no intent to cause harm. Examples include the accidental deletion of critical information, a misconfiguration of a security system that introduces new vulnerabilities, or the unplugging of a device from its power source.

Environmental threats are commonly associated with natural disasters, such as earthquakes, wildfires or flooding, but also include threats such as pandemic events[33] that could impair an organization's ability to provide a critical service. Even solar phenomena such as sun flares represent an environmental threat to Smart Grid.

Threats seek to exploit **vulnerabilities** or weaknesses in the system. Vulnerabilities can also be divided into three categories: technological, process-related, and behavioral. There are several places vulnerabilities could potentially develop in a Smart Grid.

---

[32] NERC-DOE High-Impact, Low-Frequency Event Risks to the North American Bulk Power System
[33] *Ibid.*

Technological vulnerabilities occur when a flaw in a piece of hardware or software is introduced (intentionally or accidentally). Cyber examples include operating system and application bugs, and system misconfigurations. Physical security examples include coverage gaps in facility video monitoring, weaknesses in physical barriers, or alarms that fail to trigger when a break-in occurs.

Process-related vulnerabilities are found in organizational processes. A business or organizational process missing critical checks and balances may be exploited by an attacker. Process-related vulnerabilities may be influenced by human behavior.

Behavioral vulnerabilities occur in human beings. Attackers will often use social engineering techniques to gain access to a facility or system through human operators rather than attempt to bypass sophisticated or hardened security controls. Users of information assets may attempt to do what is convenient rather than what is necessary to conduct business in a secure fashion. Such vulnerabilities can be particularly challenging to detect or measure.

Finally, the potential **impact** caused by the loss of an asset, whether the loss is related to availability of the asset, or the loss of integrity or confidentiality of information stored, processed or transmitted by the asset, must be considered in risk decision-making processes. Assets that are less critical to the operation of the Smart Grid may require fewer protections than assets that are significantly more important to its safety and reliability.

When considering threats and vulnerabilities strategically, the primary role of SDG&E's security program must be to proactively reduce the overall risk to Smart Grid that minimize the quantity and severity of vulnerabilities found in the system, whether they are technological, process-related, or behavioral; and to respond quickly to contain threats that do materialize before they can severely impact the system.

5.3 PRIVACY AND SMART GRID

SDG&E understands that the full benefits of Smart Grid cannot be achieved if it does not have the confidence of the users of the system. In particular, it is imperative that the privacy of customers' personal information and usage data be protected from all unauthorized access, disclosure or modification.

SDG&E intends to adapt several aspects of relevant guiding principles into its customer privacy framework. For example, SDG&E supports the four dimensions of privacy as described by NIST and the Fair Information Practice (FIP) principles developed by the Federal Trade Commission as key components of its security and privacy programs. In addition, SDG&E also supports other guiding principles from a process and technology design perspective, such as the Privacy by Design Seven Foundational Principles.

NIST describes four dimensions of privacy that SDG&E will consider how to integrate with its Customer Privacy Program:

"Privacy relates to individuals. Four dimensions of privacy are considered:

(1) Personal information— any information relating to an individual, who can be identified, directly or indirectly, by that information and in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural, location or social identity;
(2) Personal privacy—the right to control the integrity of one's own body;
(3) Behavioral privacy—the right of individuals to make their own choices about what they do and to keep certain personal behaviors from being shared with others; and

(4) Personal communications privacy—the right to communicate without undue surveillance, monitoring, or censorship."[34]

Further, SDG&E agrees with the seven principles set forth by Privacy by Design, namely:

1. Privacy is Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default
3. Privacy Embedded into Design
4. Full Functionality – Positive-Sum, not Zero-Sum
5. End-to-End Lifecycle Protection
6. Visibility and Transparency
7. Respect for User Privacy

"Customer privacy is becoming an integral part of the business culture within SDG&E."

These characteristics and principles become important as part of a baseline of industry understanding and best practices as SDG&E goes forward in the evolution of its Customer Privacy Program. This effort will permeate every part of SDG&E's customer privacy framework. It will positively influence the way SDG&E offers services to its customers by building confidence and trust.

However, SDG&E recognizes that the challenge of translating these principles into practice in a consistent and cost effective manner. For example, the privacy principle of "data minimization" is a worthy goal to achieve, but how this principle will be consistently applied to ever-changing innovative Smart Grid-enabled service offerings has yet to be fully determined.

[34] From "Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid"

5.3.1 EVOLVING THE CUSTOMER PRIVACY PROGRAM

Customer privacy is becoming an integral part of the business culture within SDG&E. The utility is working to tightly integrate privacy safeguards into relevant business processes and its Security Programs. Customer information privacy impact assessments and analysis of new and pending legislation, as well as maturing best practices regarding privacy will result in changes to company policy, guidelines, processes, procedures—including changes to security requirements, architectural principles and design standards, and system configurations—in order to better support customer privacy throughout end-to-end business process and technology implementations.

SDG&E will seek to minimize or eliminate the collection of unneeded customer information, share just the required customer information with only those that have a need to know, and ensure appropriate security controls protect customer information through the information's lifecycle.

Automated and pervasive data loss prevention capabilities will allow the company to minimize the risk that sensitive information could be intentionally or accidentally mishandled (i.e., printed, e-mailed without encryption, etc.) according to legal, regulatory or company security requirements.

Most importantly, SDG&E will continue to raise the awareness of privacy issues and educate employees and contractors about the necessity of respecting and protecting customers' privacy.

The Customer Privacy Officer will oversee these activities and has overall accountability for insuring the adequacy of all customer privacy controls.

5.4 ALIGNMENT TO SECURITY GUIDANCE DOCUMENTS FROM NIST AND OTHERS

As stated in the Smart Grid Deployment Plan security vision, SDG&E believes it is critical that Smart Grid is aligned with industry standards and best practices. A widely

recognized set of security standards that SDG&E uses throughout its security programs is maintained by the National Institute for Standards and Technology (NIST).

NIST represents just one set of standards and best practices that SDG&E must look to for guidance. In addition, several regulatory bodies issue standards and requirements that the company must also comply with, including the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP), the California Privacy Breach Notification Act, Sarbanes Oxley, and others. Some of these standards are duplicative, or rarely, conflicting.

To meet the challenge of complying with this growing list of standards, requirements and best practice guidelines in a sustainable and efficient way, SDG&E's security program is strategically consolidated and articulated in its unified security controls framework. SDG&E manages a master catalog of security requirements and controls that is maintained by this security program. These requirements and controls are normalized or standardized in a language that can be understood by the business as well as auditors and are not intended to be specific to any one regulatory body or set of security standards. Regulatory standards, requirements or industry best practices are incorporated into this catalog by a simple mapping exercise. Adding a new set of regulatory requirements, standards or industry best practices is a matter of mapping them to this normalized catalog of controls. In cases where a new requirement introduces a gap in the catalog, the program engages a process to define, design, test, and implement new controls quickly to ensure the new requirement can be met.

To see an example of how SDG&E uses this framework to align with the Security Profile for Advanced Metering Infrastructure, the Catalog of Control Systems Security, and the Department of Homeland Security (DHS) Cyber Security Procurement Language for Control Systems, see appendix in section 4.11.1.

SDG&E regulatory performs internal self-assessments of its compliance with required federal standards regarding security of critical infrastructure as part of its ongoing

compliance activity. Internally, the utility's compliance with these standards is reviewed, documentation and other evidence of compliance are examined, and where necessary changes are made to mitigate any areas where security can be improved.

5.5 SDG&E'S GRID AND CYBER SECURITY STRATEGY

SDG&E's security strategy aligns with the company's overall obligation to ensure the safe and reliable delivery of energy to its customers.

In order to realize its security vision, SDG&E will act on a strategy which can be summarized based on five components:

- Adhere to Security Principles
- Broaden Awareness (to Employees, Third Parties and Customers)
- Converge Security Governance
- Disaggregate Security Controls
- Comply with Federal Critical Infrastructure Protection Standards and Requirements

5.5.1 ADHERE TO SECURITY PRINCIPLES

At its highest level, SDG&E's security strategy seeks to apply fundamental security principles to its Smart Grid infrastructure.

- Minimize the attack surface of Smart Grid infrastructure components, rendering them more resistant to attack. Every system and every application must begin in a known and trusted configuration so that in the rare instance that an unauthorized change does occur, it may be quickly identified and acted upon.
- Protect customer privacy by limiting the amount of information collected about customers to that which is necessary to meet service needs while complying with all legal and regulatory obligations. Privacy must be the default, meaning that

customers will opt in or explicitly authorize the utility to share information rather than being required to opt out.

- Separate mission critical duties to minimize the risk of a single individual misusing a system or process to harm the Smart Grid.
- Simplify the management of access to critical systems to minimize the risk of human error in the application of access and to manage accountability of Smart Grid actor actions (i.e. logging critical transactions) by applying the principle of role-based access control.
- Minimize the risk that the failure of any one control leads to a compromise or failure of the system by applying defense-in-depth techniques, in which multiple layers of defense are placed throughout its systems and potential security vulnerabilities are addressed at multiple layers including personnel, technology and operations for the duration of its systems' life cycles.
- Ensure the Smart Grid is aligned with accepted security standards and best practices in order to maximize flexibility in handling the latest threat vectors.
- Separate the application of centrally managed security controls, from security controls which are distributed in the Smart Grid environment.

5.5.2 BROADEN AWARENESS

Beyond the current involvement of utility employees and contractors in security activities, SDG&E considers three different perspectives of awareness in its security strategy.

- *Develop Situational Awareness*

  A resilient Smart Grid is able to self-measure and self-assess the consistency of its security controls and their effectiveness in near real time. Security personnel monitor for and detect a broad range of physical, cyber and hybrid security events, including incidents and vulnerabilities, responding faster and more efficiently based on the priority of each.

- *Smart Grid Participant Awareness*

  Security is not only embedded into Smart Grid operational processes and technologies, but also in the thoughts and habits of the people that participate in the generation, transmission, distribution and consumption of energy, including utilities, third parties and customers. Risk owners include physical and cyber security risks in their decisions. Utility employees, third parties and customers are informed and understand the shared obligation to protect every individual's privacy and security.

- *Collaborative and Regulatory Awareness*

  Legal and regulatory compliance is more easily managed and verifiable in a complex and rapidly changing regulatory environment where transparency builds trust. The communication of relevant security information, including threats and potential vulnerability mitigations, among a larger collaborative community facilitates finding and resolving potential problems faster.

5.5.3 CONVERGE SECURITY GOVERNANCE

Convergence takes on three perspectives in this deployment plan.

- *Centralized management of company physical and cyber security capabilities.*

  SDG&E centrally enforces its security management functions and reduces the number of unique management interfaces required to monitor and control these capabilities. Security capabilities are policy driven to support the consistent implementation of security controls, large scale enterprise management through the use of automation for enterprise-wide configuration management, and remote security management. Company security processes, such as incident response, are integrated so that when an incident occurs, the company responds quickly and effectively.
- *Integration of company and third party security capabilities.*

Security capabilities are federated for company-to-third-party interoperability. Third parties may include customers, vendors, contractors, regulators or law enforcement. This provides relevant actors access to more information in order to make risk decisions. This convergence makes possible the advanced data integrity and non-repudiation capabilities required for making such large scale systems trustworthy.

- *Leverage standards*

  Diverse proposals for standardization regarding the interaction between Smart Grid systems and security capabilities unite into a single well developed and widely accepted library of standards, making interoperability between different entities cost effective, flexible, easy to manage, and secure.

5.5.4 DISAGGREGATE SECURITY CONTROLS

Disaggregated Smart Grid security controls, enforcement mechanisms, and information repositories are physically and logically distributed throughout utility operations. This approach increases the grid's resilience in the face of man-made or natural disasters. Risk management decisions sit more closely to the appropriate risk owner and are therefore, based on information provided by the sources closest to the issue. Improved automation also allows for risk decision processing with greater control by risk owners but with less human intervention.

Information security capabilities continue to evolve beyond well-known and mature network layer controls into the application layer, increasing reliance on business logic to make near real-time security decisions.

Disaggregated security capabilities support distributed security controls, enforcing decisions governed by enterprise policy while taking into account local business needs; are configured to defend local information assets without requiring access to centralized systems; and target specific localized threats.

5.5.5 COMPLY WITH FEDERAL CRITICAL INFRASTRUCTURE PROTECTION STANDARDS AND REQUIREMENTS

SDG&E seeks to maintain compliance with federal Critical Infrastructure Protection (CIP) standards and requirements at all times and continually seeks to enhance its compliance activities. These federal standards are designed to protect those assets that are critical for the reliable operation for the bulk power system.

- Compliance with federal CIP is given high priority with-in the company with a senior manager (Vice President Level) designated to as the chief manager responsible for the companies critical infrastructure protection standards compliance across the various business units.

- SDG&E has an internal Reliability Compliance department that works with the business units to maintain compliance. This department also directly reviews documentation of compliance and provides management with an independent view of the compliance activities with each business unit.

- Each business unit with Critical Infrastructure Protection responsibilities, including both cyber and physical security are internally reviewed for compliance as part of the process of self-certification of NERC reliability standards compliance.

- SDG&E continually seeks to enhance CIP Standards compliance and to ensure that its employees and contractors are well versed in the importance of compliance with these rules in maintaining the security of the grid.

As deployment develops some Smart Grid assets will be deemed to be critical and fall under the CIP Standards. SDG&E will incorporate these assets into its ongoing compliance activities and ensure that as deployment progresses these assets are afforded, at a minimum, the protections required by these Standards.

5.5.6 SMART GRID SECURITY STRATEGIC EXPECTATIONS

To meet these challenging demands of securing the Smart Grid, SDG&E must set clear security expectations across the utility and with its stakeholders, implement protocols to relentlessly monitor its systems for undesirable behavior, create a culture and technological platform that enables the utility to quickly react to potential incidents before they can cause great impact, and develop communications mechanisms to keep every relevant stakeholder informed. Grid and cyber security should also enable flexibility and extensibility to meet changing business requirements.

Cyber security will continue to use and expand network layer security controls where they provide value, and will aggressively develop application layer controls in order to meet the latest security challenges.

Ensuring data integrity will become increasingly important in a Smart Grid environment where price signals or system commands may be sent, received and acted on in more automated ways. Further, non-repudiation (assurance of data authenticity) will become essential to Smart Grid participants in order to be able to trust that other participants cannot deny their role in a given transaction.

From a physical security perspective, SDG&E will further improve its anomaly detection capabilities; including enhanced video capture, storage and retrieval, motion sensing, electronic signal detection, and physical access control technologies further into the field. It will exploit role-based and provisioning/de-provisioning capabilities in order to improve the accuracy and timeliness of physical access control.

In addition, SDG&E will consider threats related to electromagnetic pulses, and natural events such as solar flares, that could disrupt the availability of the grid.

SDG&E will act in the following ways to execute its security strategy and achieve its security vision for Smart Grid:

- Apply a “secure by design” approach
- Distribute security controls and make them more autonomous
- Develop new security capabilities to support the Smart Grid
    - Information sharing services with collaborative partners
    - Large scale situational awareness capabilities
    - Large scale information integrity and non-repudiation services
    - Endpoint protection capabilities
- Evolve existing security capabilities to support the Smart Grid
    - Community-centric security awareness capabilities
    - Internal security standards and testing capabilities
    - Software development lifecycle management
    - Enterprise logging services
    - Vulnerability management services
    - Risk and compliance management services
    - System configuration management capabilities
    - Cyber threat detection, alerting and response capabilities
    - Physical threat detection, alerting, and response capabilities
- Unify shared security capabilities
    - Integrate physical and cyber security capabilities
    - Identity and access management services
    - Encryption key management services

5.5.7 APPLY A “SECURE BY DESIGN” APPROACH

Security is more effective and less expensive when it is considered from the beginning of a project, rather than added on after the project is complete. Security controls that are designed alongside system functionality (as part of the IT lifecycle for technology projects) are more effective at protecting information and systems. It is also less expensive in the long run to design security from the beginning rather than attempt to

add security features late in the design effort, or worse, after the system or device has been deployed and placed into operations

The success of a "secure by design" approach is as much about the culture of the security within organization developing a solution as it is about the processes or technologies it deploys.

5.5.7.1 DISTRIBUTE SECURITY CONTROLS, AND MAKE THEM MORE AUTONOMOUS

For a variety of performance and reliability reasons, security controls that have traditionally been placed in data and/or control centers will move closer to the field systems that they support or be able to reach such field systems that are closer to the edge, or the consumer's residence or business. Some examples of such controls include, but are not limited to: authentication; authorization; encryption; event logging and correlation; intrusion prevention; and physical access controls such as remote cameras, motion detectors, and facility entry systems.

5.5.7.2 DEVELOP NEW SECURITY CAPABILITIES TO SUPPORT THE SMART GRID

Share information with collaborative partners

A Smart Grid introduces a new set of challenges in large scale cyber security situational awareness. Since no one organization or individual owns, operates, monitors or uses the entire grid, it is incumbent on utilities, third parties and customers that participate in its operation to share information in order to maintain a "big picture" view of system conditions, and in particular, threat activity and security events that could be indicative of a cyber attack.

SDG&E will define the set of actors (i.e., information providers or consumers of information, based on role) with which it will send and/or receive relevant information and ensure individuals in those roles receive the appropriate background checks to handle sensitive information, determine the view or set of

information that is required by each actor, develop mechanisms to collect and handle the required information, including systems and facilities that meet government sensitive information requirements, and implement resistant and resilient mechanisms to deliver the information. SDG&E's model will be modular for portability and standardized for more efficient integration with future security threat and event information actors.

Large Scale Situational Awareness Capabilities

Similar to the power system itself, increasing volumes of security event data will be captured and analyzed, so security personnel must have more efficient ways of visualizing and finding patterns, drilling down for more details, and formulating and acting on a response. Especially in physical security, augmented reality will be considered for enhancing real-time video to define and visualize security tolerance boundaries. Augmented reality may also prove invaluable by discovering hard to spot patterns in video, such as partially hidden or camouflaged objects.

Large Scale Information Integrity and Non-Repudiation Services

Smart Grid will depend on the ability for thousands, tens of thousands and perhaps millions of actors to reliably conduct rapid and frequent automated business transactions. Each actor must be able to consistently trust that the information they use to make energy decisions is being provided by a trustworthy source and that the information itself is free from unauthorized modification through the entire transaction.

Information integrity and non-repudiation services will require standardized enrollment interfaces and provisioning mechanisms. These services must seamlessly interoperate with third parties.

Endpoint protection capabilities

Endpoints generally include any device that is at the end of a Smart Grid transaction, such as a smart meter or other smart device. Depending on the role of the endpoint, it may require specific protections around authentication, authorization, least privilege oriented role-based access control, data loss prevention, malware prevention, digital rights management, or cryptographic capabilities. Legacy endpoints (i.e. existing devices that are already deployed in the infrastructure) may not be able to support modern authentication, authorization, encryption, or other capabilities. Such endpoints must still be able to securely interoperate with other endpoints on the Smart Grid network. This may require abstracting the security features that cannot be performed by the legacy endpoint to "security layer" technologies that handle these features on behalf of the legacy device.

5.5.8 EVOLVE EXISTING SECURITY CAPABILITIES TO SUPPORT THE SMART GRID

Community-Centric Security Awareness Capabilities

Cyber security is an issue about which people are relatively aware and concerned. SDG&E can leverage that awareness and enhance it by collaboratively sharing knowledge, best practices and experiences with its customers, partners, regulators, and employees.

Communicating regularly with this larger community is a priority for SDG&E and includes such topics as threat information and privacy concerns. Awareness programs the utility is developing will be pervasive, deliver a consistent message, multiple times and over a variety of delivery mechanisms, both physical and electronic. SDG&E will also be prepared to receive information about threats and vulnerabilities and distribute this information quickly to the affected parties.

Cyber security cannot be relegated to the back office. Those with a responsibility to secure information must play an active and communicative part in making this

larger community aware of the current state of the SDG&E's security posture as well as allowing this larger community to keep the company aware of its ideas and concerns on any planned future state.

Internal Security Standards and Testing

Standards are critical to the development of strong and repeatable security controls, and in the measurement of their effectiveness. Without standards, interoperability becomes increasingly difficult and prohibitively expensive. SDG&E participates in a variety of industry and Smart Grid standards organizations in order to improve security capabilities while ensuring compliance with industry-accepted standards.

SDG&E will invest in security testing against new and existing field embedded and wireless systems, and in the performance of regular reassessments of existing systems deployed in the operational environment to quickly find and mitigate vulnerabilities.

Software Development Lifecycle Management Services

Smart Grid will require significantly more software components than the aging infrastructure it will replace. While much of this software will be produced by third parties, SDG&E will evolve its capability to produce and maintain quality software that is free of defects and security vulnerabilities. Existing software management processes will be unified and integrated into a single well-managed and authoritative capability.

An enterprise software development lifecycle management capability will include the technology, processes and organizational units required to effectively and repeatedly write software; thoroughly check it for defects; and ensure its integrity through development, unit testing, deployment and while it remains in production.

Further, this management capability will be prepared to incorporate third party software, including source code if available and necessary, that is introduced into company environments.

Lifecycle management capabilities should make it easier for software developers to focus more on software development while meeting relevant software security standards.

Enterprise Logging Services

Enterprising logging is the heart of event collection for actor accountability, anomaly detection and incident response automation. The utility must be able to store much more event data in a scalable fashion and process that data faster for delivery to various monitoring, correlation, and compliance tools.

Vulnerability Management Services

Vulnerability detection and response capabilities must have wider reach across more systems and discover more vulnerabilities in near real time. These capabilities will include traditional vulnerability discovery tools like vulnerability scanners that conduct sweeps of an environment, as well as querying tools that examine system configurations, and passive tools that observe passing network traffic in order to infer potential vulnerabilities.

Vulnerability management will begin examining systems that in the past have had little or no cyber footprint, such as SCADA systems and field equipment, in order to find vulnerabilities in these specialized devices.

Risk and Compliance Management Services

The calculation of physical and cyber security risk must become quantifiable and reliable. Risk owners must be able to depend on risk data for their decisions. Risk data must be available to risk owners via their preferred delivery mechanisms.

SDG&E will be able to measure more frequently and report more quickly to multiple stakeholders, both internal and external.

Compliance Management

Documentation, reporting and visualization of controls objectives, controls and associated risks, surveys and self-assessments, testing, and remediation is a necessary feature of compliance management. Compliance management should support various types of compliance, such as ISO 27002; NIST 800-53; and other standards, industry-specific regulations such as NERC Critical Infrastructure Protection (CIP); service-level agreements; trading partner requirements and compliance with internal policies. Testing, verification, and measurement of control effectiveness are critical to assure continued compliance.

Risk Management

Risk is managed by the documentation, assessment, gap analysis, reporting, visualization, and remediation of risks. The risk management framework should provide a structure of capturing potential issues found during assessment and analysis, reusable controls for remediating risk, and reporting capabilities to ensure the risk owners are aware of their risk posture.

System Configuration Management Capabilities

Any change to a production system should be recognized, authorized and documented. Unauthorized changes should be immediately apparent and operators should have the ability to revert to a trusted state remotely and in a trusted fashion with minimal interaction. Systems should recognize and reject attempts to modify logical components. In some cases, even if software delivery controls are circumvented, the system should be able to recognize an

unauthorized change and revert to a previous trusted state without human intervention.

Cyber Threat Detection, Alerting and Response Capabilities

Collecting event data is not enough. Event data must quickly be analyzed for known patterns and anomalous behavior. The company must enhance its monitoring, detection, and response capabilities to provide for more automated defense mechanisms and security personnel augmentation capabilities. Threat analysts and responders must leverage visualization technologies that allow them to visually consume and interact with potentially millions of security events per hour.

From a cyber perspective, this means improving intrusion detection and prevention, and data loss prevention capabilities. Grid computing which harnesses the power of underutilized computer processors to perform process-intensive tasks will be considered for threat analysis.

These cyber security threat capabilities must integrate with relevant physical security capabilities in order to gain a better understanding of large scale or blended threats.

Physical Threat Detection, Alerting and Response Capabilities

The company must expand its facility and property surveillance from existing visible light technologies into the thermal, infrared and low visible light spectrums. Capabilities are required to detect and respond to anomalous electronic signals that could indicate potential information gathering or sabotage threats.

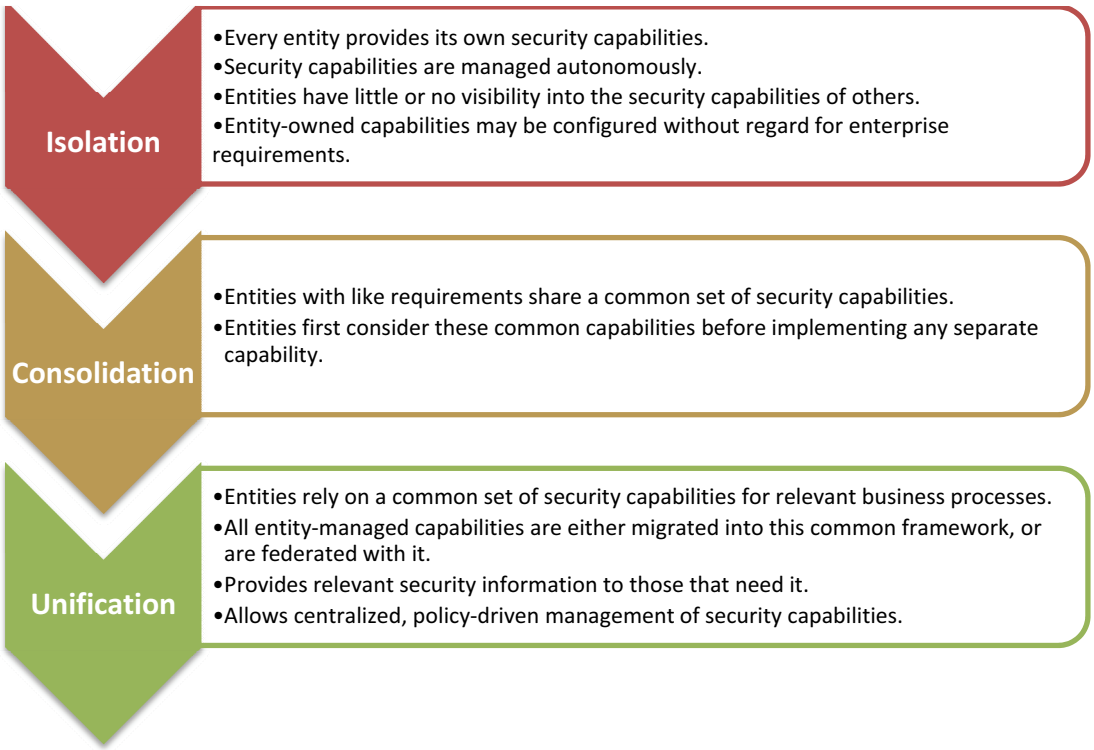
Further, the company must be able to monitor increasing numbers of local and remote facilities and equipment, be alerted to anomalous events, recognize physical security threats, and quickly respond.

Finally, these physical security threat capabilities must integrate with their cyber cousins in order to gain a better understanding of large scale or blended threats.

5.5.8.1 UNIFY SHARED SECURITY CAPABILITIES

Company security organizations, technologies and processes, including security risk management, event monitoring, incident handling, provisioning, de-provisioning, authentication, authorization and encryption must be able to be managed and monitored from a more centralized security perspective. Specific entities, such as business units or third parties, may have specific requirements for their business areas, but these requirements should integrate cohesively with the larger security directive to minimize risk without sacrificing flexibility. Such capabilities should allow the company to work with third parties, regulatory agencies, or collaborative community-driven needs to share information. The following diagram depicts the various levels of maturity in shared security capabilities.

Figure 5-1: Maturity Levels of Shared Security Capabilities



Integrate Physical and Cyber Security Capabilities

The threats that face a Smart Grid are relentless, having the luxury of time and unlimited cumulative resources on their side. As these threats already operate both in the physical and cyber worlds simultaneously, so must the company's security program combine its physical and cyber security capabilities in order to detect, prevent, and when necessary, respond to, such threats in a coordinated and well-practiced fashion. SDG&E will manage these capabilities under a centralized joint security operations center (JSOC).

Identity and Access Management Services

All actors, including user, systems, and some applications, must have unique identities in order to conduct secure transactions on a Smart Grid. This capability must incorporate externalized authorization, coarse- and fine-grained role-based access control, and federation with internal as well as third party systems, and with cryptographic key management systems. Multi-factor authentication will be required for users of the system in specific roles, circumstances, or threat conditions. Further, authentication, authorization and access control mechanisms must become more centralized for more consistent management and support multiple levels of granularity.

Encryption Key Management Services

Strong information integrity and non-repudiation services will require a centralized and unified key management system in order to protect valid encryption keys and revoke those that have expired or become compromised.

5.6 SDG&E'S INFORMATION SECURITY PROGRAM

This section of the Smart Grid Cyber Security Deployment Plan describes the Information Security Program for the company. The security program addresses

information security in the broadest scope and determines SDG&E's methodology for following its security strategies.

As part of implementing its Smart Grid security strategy, the company will apply its Information Security Program, including the following elements.

- Information Security Governance
- Information Management
- Compliance Program
- Security Awareness and Training
- Security Strategy and Architecture
- Security Principles in Contracts
- Information Security Engineering in the System Development Lifecycle
- Operational Security

5.6.1 INFORMATION SECURITY GOVERNANCE

Company information security governance practices support the effective operation of the company in carrying out its role as a public utility with the verifiable assurance that information assets are handled in a manner that protects the business and is consistent with applicable laws and regulations.

Management of any complex system such as those required to deploy SDG&E's Smart Grid vision requires well documented and understood accountability and responsibility of a system's "users" and owners of the system. The company's Security Governance Program includes the following elements.

- Leadership: Define roles that are accountable and responsible for protecting information and information assets. These roles provide the appropriate level of authority necessary to execute their responsibilities.
- Requirements in a comprehensive security policy framework.

- Partnerships: Partnerships with external stakeholders, including law enforcement and regulatory entities, to facilitate reporting and escalation of important security incidents and information securely and efficiently.
- Risk Management: No organization can protect everything with the same level of security, nor should it. Risk based management of security includes a value and impact-based methodology to ensure protections are commensurate with the value of the asset being protected.

5.6.1.1 INFORMATION SECURITY LEADERSHIP

The company's Information Security Program defines leadership roles and responsibilities to fulfill key activities and decision making within the program. The key roles are those of information and system owners, security professionals, and operations and system administration staff. Smart Grid technology deployments will be subjected to this program element as part of SDG&E's ongoing best practices in security leadership and decision-making.

The corporate structure consists of Officers, Directors, Managers, and Staff.

For example, specific Information Security Program roles include:

- The Chief Information Officer has overall accountability for the information security posture of the company and its information assets.
- The Director of Information Security and IS Compliance has the overall responsibility for company Information Security department activities.
- Managers address aspects of strategy, architecture, compliance, risk, governance, engineering, and operations.
- Various staff positions provide multiple support functions to company projects, assisting in design, implementation, operation, management, and compliance activities.

- A Computer Incident Response Team (CIRT) is responsible for detecting, responding to, and assisting in the recovery from computer security incidents that impair the company's ability to conduct normal business operations.
- Information Security Advocates (ISA) participate in a cross functional team comprised of business, IT and security team members. ISA's are a practical extension of the enterprise security program into the business.

5.6.1.2 COMPANY INFORMATION SECURITY ROLES AND RESPONSIBILITIES

An individual may be assigned to one or more of the following roles. Each role has specific responsibilities with respect to information security and protecting company assets. Table 5-1 lists those roles & responsibilities:

Table 5-1: Security Roles & Responsibilities

Role	Description
User	An individual who accesses or attempts to access Company Information and/or Information Systems.
Risk Owner	Company officer or executive that is ultimately accountable for risk and has the ability to assume financial impact of an accepted risk or the residual risk related to the outcome of a risk treatment. In many cases, the Risk Owner can also be the Information Owner.
Risk Manager	Company executive or director that has been delegated a limited level of responsibility for making risk decisions on behalf of the Risk Owner.
Control Owner	Directors or managers ultimately accountable for security controls. Control Owners report to Risk Managers any deficiency of controls related to the protection of company information and information systems. Control Owners don't necessarily need to organizationally report directly to a Risk Manager.
Control Manager	Individuals responsible for implementing and maintaining operational controls. A secondary responsibility exists to ensure controls are operating effectively and performing as expected. Control Managers are assigned by and report deficiencies to Control Owners.

5.6.1.3 POLICY FRAMEWORK

Company security policy documents are organized by artifact type. Company security policy artifacts include:

- Policies: The set of business rules and practices that regulate how an organization manages and protects sensitive information.
- Guidelines: Provide practical direction for what people need to do in order to comply with security policy.
- Standards: A specification of agreed security features and controls that are established for use within the company.
- Procedures: Detailed step-by-step instructions that define how to perform information protection processes and activities.
- Requirements: The specifications of the security features and controls necessary to satisfy security policy.

Company Information Security policies are based on accepted standards and guidelines, including ISO 27002 and the NIST 800 series standards, and cover regulation important to SDG&E, such as NERC CIP Standards and Requirements and many others. The policy framework applies to the Sempra Energy Utilities (SEU), including SDG&E and the Sempra Energy Corporate Center (CC).

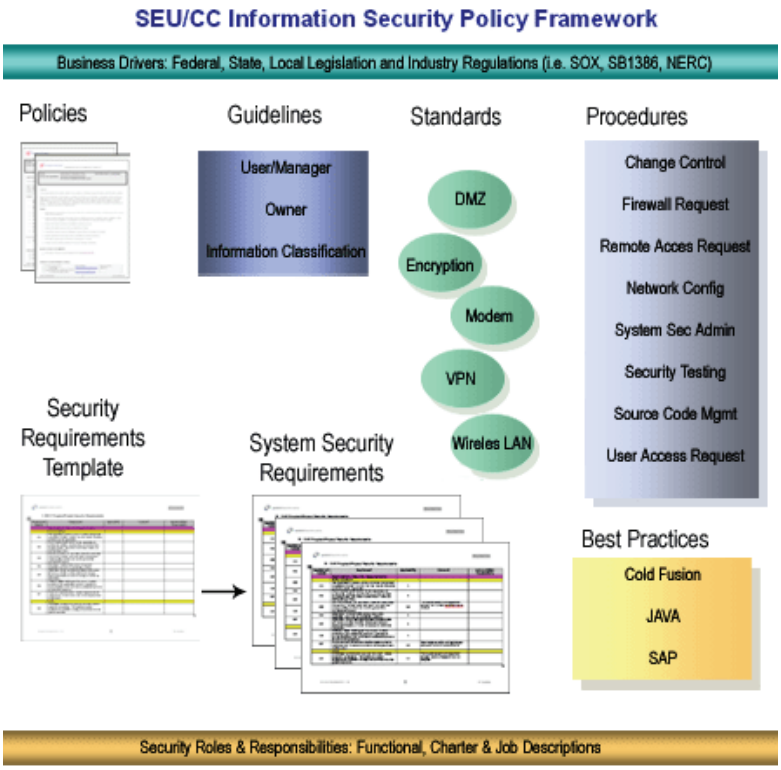


Figure 5-2: SDG&E (SEU/CC) Information Security Policy Framework

5.6.1.4 EXTERNAL PARTNERSHIPS

The Information Security team maintains a number of partnerships outside of the company. The partnerships include industry groups, community organizations, and state and federal organizations. Best practices in Smart Grid cyber security, physical security and privacy will be shared with these groups by SDG&E where appropriate and SDG&E expects to work collaboratively with these external partners to accelerate best practices throughout the industry as it implements its Smart Grid vision.

Some of the industry groups include:

- UCAIug/Open Smart Grid User Group
- GridWise Alliance/Interoperability and Cyber Security Working Group
- ZigBee Alliance

- EPRI
- International Information Systems Security Certification Consortium, Inc. (ISC)[2]
- Information Systems Audit and Control Association (ISACA)
- Information Systems Security Association (ISSA)
- UTC (Utilities Telecom Council)

Activities with community, State, and Federal organizations include:

- DOE/NIST Smart Grid Cyber Security Working Group
- DHS Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) security briefings
- Federal Bureau of Investigation (FBI)
- Western Electricity Coordinating Council (WECC) Critical Infrastructure Protection User Group
- Electricity Sector Information Sharing and Analysis Center (ES-ISAC)

Partnership with other industry experts:

- Active participation and information sharing with local companies in the financial, healthcare and other industries;
- Active participation with various industry peer groups – CISO, CSO Round table, etc.

5.6.1.5 RISK MANAGEMENT & ASSESSMENT

Enterprise Information Risk Management is an ongoing process to proactively manage risk related to information assets. Its objectives will be applied to new Smart Grid deployments to manage risk, make information risk decisions, drive awareness of potential risk impact and ensure continual assessment, measurement and process improvement:

- Provide the company with a standard framework for managing information risk;

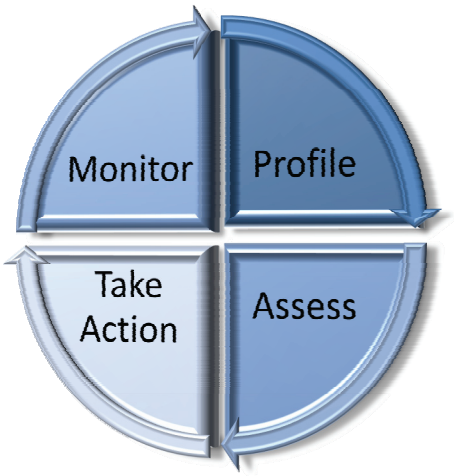
- Provide the ability for the business to make informed information risk decisions;
- Make the company aware of the potential risk impact to its information;
- Continual assessment, measurement and process improvement.

These objectives are accomplished using an Enterprise Information Risk Management (EIRM) framework and information assurance process that is aligned with the company's core values and risk tolerance, in order to assess and manage information risk.

5.6.1.6 EIRM FRAMEWORK DEFINITION

The four key phases of the EIRM Framework are depicted graphically, as well as described below:

Figure 5-3: Enterprise Information Risk Management Phases



- ***Profile***: identifies company information assets and their value.
- ***Assess***: provides threat classification and security vulnerability information, along with potential business impact, to suggest possible responses to different categories of information risk.
- ***Take Action***: empower business managers to make informed decisions to prioritize risks and implement appropriate controls.

- ***Monitor***: ensures that current and future risks can be minimized through ongoing maintenance and monitoring activities.

5.6.2 INFORMATION MANAGEMENT

Information Management consists of creating, handling, and when necessary, securely destroying data throughout its lifecycle as required by the company records retention policy and applicable law or regulation, as well as appropriate handling and disclosure required by information sensitivity, legal and regulatory requirements. Information is classified based on its value and sensitivity combined with the impact of its loss, modification, or unintended disclosure. Company records are a specific type of information with additional handling requirements.

5.6.2.1 INFORMATION CLASSIFICATION

Company information is categorized into one of four classification levels. The classification levels do not affect any privilege status or preclude the use of more stringent need-to-know restrictions for the dissemination, protection, and use of the information.

The four categories are “Public,” “Internal,” “Confidential,” and “Restricted.” These categories are applied to Information or data, commands, and controls for all forms of systems. Roles and responsibilities are defined for information to determine the appropriate classification and handling of specific pieces of data.

- **Public Information** – Public Information is any non-privileged information prepared, owned, used, or retained by the company and that is required or intended to be disclosed or made available to the public. Public information must be authorized for release prior to being released to the public domain.

- **Internal Information** - Internal information is generally releasable to Company employees and contractors designated by an authorized employee to receive such

information, subject to privilege and/or need-to-know restrictions. It requires a degree of protection because unauthorized acquisition, modification or destruction of internal information could result in loss of productivity, disruption of Company operations or negatively impact the company's reputation. When a handler is unsure of a piece of information's classification, it should be assumed to be, at a minimum, Company Internal information.

The external release of internal information regardless of the transmission media must be authorized by the information owner.

Unauthorized release of Company Internal information could:

- Reduce Company competitive business advantage;
- Increase the risk profile of the company due to attacks;
- Tarnish the reputation of the company;
- Negatively impact service availability and/or reliability.

- **Confidential Information** – Confidential Information is any information that if disclosed or corrupted in an unauthorized manner could cause *great* harm to an individual or the company. It requires reasonable control because unauthorized access or improper security measures could cause a violation of applicable law or could harm the company's reputation, credibility, competitive advantage, revenue generating potential or employee morale.

  Dissemination of Confidential Information regardless of the transmission media must be authorized by the Information Owner.

  Unauthorized release of Company Confidential information may significantly:

  - Compromise the company business reputation and credibility;
  - Increase the risk profile of the company due to attack;
  - Decrease Company competitive business advantage;

- Reduce Company revenue generating potential;
- Destroy employee morale.

- **Restricted Information** – Restricted Information is any information that if disclosed or corrupted in an unauthorized manner could cause *extremely grave* harm to an individual or the company. It requires maximum control because unauthorized access or improper security measures could cause an impairment of business activities or significant economic damage and/or significantly damage the health and well-being of individuals, and may also cause a violation of applicable law.

  Restricted information requires explicit written approval dissemination by the information owner, including off-site records retention.

  Unauthorized release of Company Restricted information would significantly:

  - Impair the ability to generate, transmit or distribute energy;
  - Harm the economic well being of the communities served;
  - Inflict irreparable harm on the general public.

5.6.2.2 NEED-TO-KNOW

The hierarchical classification may not always be sufficient to adequately determine the appropriate protection measures for information. Reasonable security features and controls should be used to protect information from misuse, unauthorized access, unauthorized acquisition, destruction or disclosure. Access to information may be further limited based on business considerations and an individual's "need-to-know." Generally, information should be limited to the fewest number of individuals to reduce the risk of compromise or misuse.

"Need-to-know" categories are often dictated by customer/employee privacy, legal, regulatory and business considerations, and typically include:

- Affiliate Compliance;

- Client-Attorney privileged Information;
- Procurement contracts during the Request for Proposal and/or preparation process;
- All personal Information protected from disclosure by applicable law.

Information which is privileged, pursuant to the Attorney/Client privilege or otherwise shall remain privileged irrespective of its classification above.

5.6.2.3 INFORMATION LABELING

Marking or labeling is the process of designating the value of information based on its hierarchical classification, any associated need-to-know restrictions and in some cases, any associated need-to-know privileges. All Company information may be marked with one of the four classifications as an advisable means of communicating such status to recipients. Company information should also be marked with need-to-know restrictions as an advisable means of communicating such restrictions to recipients. Privileged Company information shall remain to the applicable privilege irrespective of whether it is marked, but the discloser may wish to mark it as such for clarity. If the classification or need-to-know restrictions/privileges of the information are unknown, employees are trained to check with their manager/supervisor, the associated information owner or the applicable records retention schedule.

Information, depending on its media, may be labeled in some of the following ways:

- Within electronic files and/or documents;
- On the media containing the Information;
- On printed or hard copy Information.

Trade Secret Marking Guidelines – Intellectual Property law recognizes patents, trademarks, copyrights and trade secrets. Trade secrets require special protection measures. The term "trade secret" under the California Uniform Trade Secrets Act

means information, including a formula, pattern, compilation, program, device, method, technique, or process, as well as contractual non-disclosure protections that:

1. Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and

2. Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Accordingly, Trade Secret Information shall be appropriately safeguarded based on its classification – Internal, Confidential or Restricted, such status can be communicated effectively by marking.

5.6.2.4 INFORMATION AND SYSTEM APPROPRIATE USAGE

Company policy defines appropriate business use in the Information Security Acceptable Use Policy to address such impacts as privacy but also guidelines for usage of information on portable devices, legal considerations and password management which will be applied to SDG&E's information produced in association with Smart Grid deployments to ensure proper usage.

- Privacy rights and employee expectations;
- User Guidelines with respect to;
- Authorized Business Use;
- Protecting Information and Information Systems;
- Password Management;
- Information Transfer;
- Legal Considerations;
- Portable devices;
- Information Retention.

5.6.2.5 RECORDS MANAGEMENT POLICY

The company retains only those records and non-records that are necessary for complying with legal, regulatory or financial requirements and for conducting business. All business units involved with Smart Grid deployments are subject to and will comply with and implement this policy. Each employee is responsible for understanding this policy and maintaining and disposing of records and non-records, regardless of media, within their possession or control in compliance with this policy.

5.6.2.6 INFORMATION DESTRUCTION

It is important information is kept (which includes company records) for as long as required to meet company policy and regulatory requirements. When any piece of Smart Grid-related information is no longer needed, it's equally important that it is destroyed according to its level of sensitivity.

Information stored in hard-copy, or on electronic media, that has been classified as confidential or restricted should be shredded or its media physically destroyed when it is no longer needed.

5.6.3 COMPLIANCE PROCESS

The Company Information Security Compliance Program oversees compliance with external requirements, internal policies and business processes. It also defines IT departmental responsibilities and monitors, measures and reports on compliance status via exception engagement / issue tracking.

The Information Security Compliance Program assists the business with compliance with the Information Security aspects in a number of business areas. SDG&E's Information Security Compliance Program ensures that all Smart Grid information security is in compliance with the regulations and statutes such as:

- Electric Reliability Standards as required by FERC (such as, NERC CIP, NERC Communications/COM);
- FERC Order 717 (Affiliate Compliance Code of Conduct);
- CPUC Affiliate Transactions Compliance (Shared V.C., D.97-12-088/ D.97-12-029);
- Consumer Information Privacy (Gramm-Leach-Bliley Act [GLBA], SB 1386);
- Breach Notification (SB 1386, California Database Breach Notification Act [CDBNA]);
- Identity Theft detection (Red Flag Rules);
- Financial Integrity (Securities and Exchange Commission [SEC], Sarbanes-Oxley Act [SOX]);
- Retention and eDiscovery (such as, Federal Rules of Civil Procedure [FRCP], CA's AB 5);
- Medical Information Protection (Health Insurance Portability and Accountability Act [HIPAA], California Civil Code 1798);
- Credit Card and Checking Account transactions (The Electronic Payments Association [NACHA], Payment Card Industry [PCI]);
- California specific (California Highway Patrol, Department of Motor Vehicles).

Roles and Responsibilities

Responsibility for the Compliance Program on a day-to-day basis resides with a variety of business and IT operating groups, particularly those areas and departments of the company affecting the confidentiality, integrity and availability of information assets. Senior Management or their delegate(s) in these departments, or areas, are responsible for communicating its compliance responsibilities to affected employees within the department and monitoring compliance with applicable standards, policies and regulatory requirements. The Senior Management or their delegate(s) will be responsible for activities, procedures and changes necessary to ensure their department, function or area is in full compliance with external requirements, internal policies and business processes.

Information Security Compliance Tools and Processes include capabilities such as:

- Controls and Policy Mapping;
- Policy Distribution and Attestation;
- IT Control Self Assessment and Measurement;
- Governance, Risk and Compliance Asset Repository;
- Automated General Computer Controls Collection;
- Remediation and Exception Management;
- Basic Compliance Reporting;
- IT Compliance Dashboards; and
- IT Risk Assessment.

Information Security Compliance Internal Controls and Monitoring

The Compliance Program proactively monitors and self–assesses its compliance with all applicable standards, policies and external requirements as well as its processes intended to ensure its compliance. SDG&E undertakes numerous compliance activities which differ in scope and activity depending on the compliance requirement, including:

- Control effectiveness review/ verification, attestation and certification;
- Periodic internal audits by Audit Services (in Sempra Energy Corporate Center) of one or more control areas;
- Periodic external audits by qualified third parties of one or more control areas;
- Ongoing monitoring of regulatory environments for development of necessary changes;
- Ongoing monitoring for compliance, control effectiveness and program effectiveness;
- Regular compliance meetings;
- Prompt and thorough assessment of compliance questions;

- Coordination and facilitation of compliance inquiries with appropriate resources within IT;
- Regular evaluation of documents, procedures and resources associated with applicable standards, policies and regulatory requirements;
- Timely investigation, assessment, risk mitigation and remediation of compliance events and issues to ensure continued compliance and to prevent reoccurrence.

5.6.3.1 RISK TREATMENT

Once the risk is understood, a Risk Owner has four options. He or she can

- Avoid the risk,
- Mitigate it,
- Transfer it, or
- Accept it.

Risk **avoidance** means the Risk Owner can opt not to continue with the source of the risk. For example, the service may not be offered, or a vulnerable system may be removed from the network.

Risk **mitigation** provides the Risk Owner great flexibility. The service may be offered, but security controls must be put in place to reduce risk to more manageable levels. For example, a vulnerable system may be patched to reduce the risk of getting a computer virus. There may be several options for risk mitigation of varying costs for the Risk Owner to consider. In the same example, the vulnerable system may also be placed behind a firewall or other network-based security control to further reduce the risk of virus infection.

Risk **transfer,** or risk sharing**,** is for situations where it may be more cost-effective to allow another entity to adopt the risk rather than for the Risk Owner to pay to mitigate or accept risk. For example, a third party hosting service may be contracted with to provide a web server if the Risk Owner has reason to believe the third party can more

effectively manage the risk of computer virus infection on its web servers. Risk transfer may also include the purchase of insurance in order to offset cost if a risk condition is realized.

Risk **acceptance** is a process in which a Risk Owner makes a decision to accept a specific security risk because the overall cost of addressing residual risk through avoidance, mitigation and/or transfer outweighs the value of the information asset(s) being protected. Risk Acceptance provides the Risk Owner an opportunity to understand and document a known Information Security Risk Situation. A Risk Owner can only accept risk for information assets they own. Only a Senior Executive responsible for the business unit at risk may assume risk on behalf of the subject enterprise environment.

Risk Acceptance is used if a company security policy, procedure, standard, or requirement cannot be met because:

- It is physically infeasible to do so (i.e., physical attribute prevents implementation of security controls);
- Logically infeasible to do so (i.e., significant impact to business process, service and or financials, or regulatory requirements);
- The cost of implementing a specific security control outweighs the value of the information asset(s) being protected.

Risk Acceptance is not permanent. The business unit and or organization must satisfy the necessary requirements and come into compliance with Information Security Policy within a designated period of time described in the Risk Acceptance.

It is the purpose of the Risk Acceptance to define the issue(s), develop a plan, and begin the path to remediation, not to become comfortable or complacent with the known risk. The Risk Acceptance process requires that a plan be submitted that identifies what corrective action(s) will be taken, when those actions will be accomplished, and who is responsible for doing them. There is a maximum duration for a risk acceptance, at which point it will have to be renewed through the same process, or the risk is demonstrated

to be remediated, or circumstances that created the risk have ended, or the acceptance has been renewed. After exceeding the period of risk acceptance, and failing remediation, or the end of the risk situation, Information Security may take steps to minimize the risk, either by adding compensating security controls, or removing the risk (i.e., shutting down a risky application or server).

When vulnerability is discovered in a third party product or service, a risk assessment is performed to assist the business in determining an appropriate course of action. Where vulnerabilities can be exploited, the business may elect to postpone implementation of the vulnerable system or proceed with implementation in acceptance of the residual risk. In both cases, vendors or service providers are informed of the vulnerabilities and asked to remediate them. Also in both cases, the conditions are tracked to remediation by the company risk acceptance process.

5.6.4 SECURITY AWARENESS & TRAINING

Security awareness and training is critical to preserving a secure Smart Grid environment. The company uses several methods used to promote awareness with a focus on role-based audiences, diverse delivery mechanisms, and relevant messages. The Company Information Security Program makes training available to employees regarding acceptable use and other aspects of the security program. Specific regulations and laws which apply to certain segments of the business provide targeted security training in those focused areas.

Security awareness and training is offered to all employees through a variety of diverse communications mechanisms in topical areas such as social engineering, password handling, managing information in their work areas, locking and securing workstations, reporting possible security issues, and facility security and safety.

Physical and Cyber security personnel receive ongoing training to maintain and expand knowledge in their fields of expertise. Training consists of security certifications,

specialized skill training, technical training on specific systems and platforms, and information security awareness.

As part of the continual improvement of the company's overall security posture, the Information Security department has established an Information Security Advocates (ISA) Program. This program helps to align business and security strategy goals by developing and maintaining a team of business-focused personnel that help establish a foundation for key business drivers, processes, requirements and impacts while distributing responsibility for select information security tasks across business domains.

Candidates are leaders within groups at the manager level or below that have an interest and willingness to learn more about Information Security and how it impacts their core business area. Participants are given a two day training course followed by a company-specific certification test. After passing the test, the ISA team meets periodically to share knowledge and experiences.

5.6.5 SECURITY STRATEGY AND ENTERPRISE RISK ARCHITECTURE

The company's Information Security Program includes the following architectural and strategic elements which will be applied to protecting the physical and cyber security needs of the Smart Grid.

- Adopt a Comprehensive View. System security design should look beyond traditional organizational boundaries, demarcation points (such as those between transmission and distribution systems) and areas of responsibility in order to work with interconnected systems and other authorized "users" to ensure security is maintained when information is exchanged between different systems or entities.
- Improve Interoperability. System components should be designed in such a way as to show how they maximize resilience, reusability and interoperability with

adjacent systems, allowing authorized interfaces to “plug and play” in trusted and predictable ways with centralized services.

- Manage Standards. Security solutions should be developed via consensus-driven security standards and development methodologies, such as those described in the NIST interagency report in order to minimize the risk that proprietary technologies will be exploited by threats while improving cost effectiveness and reliability.
- Balance Redundancy. Systems should be designed in a cost-effective way to minimize the chance of a single point of failure causing adverse impact to the overall system.

5.6.6 SECURITY REQUIREMENTS IN CONTRACTS

Key security requirements are embedded in contracts with vendors and service providers. The general contract areas, below, are augmented with specific requirements based on the specific product or service addressed by the agreement. The contract language requires verifiable accomplishment of security goals and adherence to security standards and best practices, and that verification may be performed by the company or a trusted third party. Contract language is intended to instill in third parties a necessary sense of urgency in protecting information assets and customer privacy. It describes third party obligations to protect information in alignment with industry accepted oversight and audit procedures. It further describes third party liability if they are the cause of a security breach.

The contracts have language regarding:

- Role Based Security Controls;
- Shared Application Architecture;
- Account Management;
- Application Interface Controls;
- Encryption;

- Password and Logon Standards;
- Data Security;
- Logging and Errors Details;
- Operational Support and Administration;
- Source Code Review;
- Vulnerabilities and Defects;
- Security Assessments and Testing;
- Right to Report.

5.6.7 SOLUTIONS DEVELOPMENT AND IMPLEMENTATION LIFECYCLE

The mission of Information Security Engineering is to provide Information Security guidance and consulting services to the Information Technology (IT) department and its clients during the preproduction phases of the system development lifecycle. This approach to information security during preproduction will assist in the "secure by design" approach SDG&E envisions for all Smart Grid technology deployments.

5.6.7.1 SECURITY ENGINEERING PROCESS TOOLS

The Information Security Engineering team uses several process tools in the course of an engagement. These tools are the Risk Triage Process, the Security Assessment Methodology, the Key Concerns for Information Security Document, the Information Security Requirements Document, the ITPL Documentation Required for Phase Review document, and the Security Evaluation Methodology.

5.6.7.2 IT SYSTEM LIFECYCLE SECURITY CHECKPOINTS

Information Security includes sign-off checkpoints at the Requirements and Design phases, and "go/no-go" authority at the Test phase of the IT System Lifecycle. Approvals are requested from Information Security by the project team, and establish

assurance throughout the System Development Lifecycle (SDLC) that Information Security Requirements are met.

5.6.7.3 SECURITY ENGINEERING PRODUCTS

While supporting the IT System Lifecycle, various artifacts are produced to communicate the developing and measured security posture of the information asset being developed.

During Project Preparation phase, the project team identifies the types of information that an asset will handle; the information owner and custodians of that information; the sensitivity of the information, and the environments in which the information will be handled and accessed. Information Security uses this information in conjunction with interviews of the project team and the various stakeholders to develop a Preliminary Risk Assessment for the information asset. This risk assessment identifies generalized risks that the asset may pose to the enterprise and the information that the asset handles, and provides recommendations on the types of controls that should be employed in protecting the information.

At Requirements phase review, the Preliminary Risk Assessment is reviewed along with the Requirements documentation to verify that the recommended controls are required as part of the project. Direct feedback is provided to the project team in order to facilitate any necessary changes to the Requirements that support necessary Information Security controls.

At Design phase review, the Design document is examined to identify if the design appears to effectively implement the required controls, and to identify any risk conditions or deficient controls that may not have been previously apparent. Direct feedback is provided to the project team in order to facilitate any necessary changes to the Design that support necessary Information Security controls.

During Build phase, the assigned Security Engineer provides direct support for implementation of security controls by the project teams. In addition, the assigned Security Engineer performs some preliminary security testing on baseline configurations of products, usually before customization and integration happen. This provides a means of identifying vulnerabilities in software or integration products that the vendors will be expected to remediate before the asset enters production. The findings from the detailed technical testing at this stage include specific identification of vulnerable conditions or material defects that lead to security risks, and are usually identified by the Common Vulnerabilities and Exposures (CVE) references maintained by MITRE Corporation.

At Test phase, the asset is tested for compliance with technical and administrative security controls. The depth and detail of this testing varies according to assessed risks, with more detailed and comprehensive testing being afforded to those assets that are assessed with the highest risk levels. The result of the Test phase review of an asset is a Security Evaluation Report that describes its overall security posture and specific steps to remediate any vulnerability findings. Information assets must be determined to be compliant with Information Security Requirements before Information Security will grant approval for an asset to enter production through Change Management processes.

Upon successful completion of Test phase, Security Engineering transitions tracking of the asset to the Information Assurance team for follow-on compliance work. The asset is tracked as a matter of course by Security Operations processes.

5.6.7.4 SECURITY ENGINEERING PRODUCTS FOR PARTNER PRODUCTS AND SERVICES

Increasingly, hardware and software solutions are outsourced to third parties that are not under the direct management of SDG&E. Often, this situation makes it impractical to apply the company lifecycle approach. To address potential differences, additional or

alternative controls are leveraged. For example, external third parties may be evaluated as accomplishing company control objectives either using direct examination by company Information Security personnel or by an independent third party.

In both cases, the subject third party is measured for compliance with commonly used standards like International Organization for Standardization (ISO) 27001, ISO 27002, ISO 15408, or NIST SP 800-53. Additionally, a previously performed comprehensive Statement on Auditing Standards (SAS) 70 type II audit may be used to collect information about the security posture of a third party.

Contract terms and clauses in the Statement of Work or Master Services Agreement provide the mechanism for enforcement of the security-related requirements and the right to measure accomplishment of control objectives.

5.6.8 OPERATIONAL SECURITY

The goal of operational security is to ensure that information and information systems are continually monitored for threats attempting to access, damage or otherwise disrupt them, and for the vulnerabilities those threats are trying to exploit. The company's Information Security Program includes the following operational security elements.

- Event Collection and Logging. Information systems forward logs and events to centralized environments for the collection and analysis of events.
- Event Management. A 7x24 Security Operations Center monitors events and logging systems for suspicious events that are detected and initiates an incident response team, as necessary.
- Incident Response. If a security event occurs, an incident response may be initiated. Suspicious events that escalate into incidents are recognized quickly, and contained in order to minimize adverse impact to the system, so recovery of the system can begin. Incident responders are readied for such activities through

training, procedural development, testing and continuous improvement. Criminal incidents are reported through the internal Corporate Security department to appropriate law enforcement agencies.

- Vulnerability Management. Vulnerabilities are identified and evaluated before they can be exploited by a threat, and to ensure timely mitigation of those vulnerabilities.
- Penetration Testing. Testing is performed in an effort to discover and mitigate vulnerabilities. Internal and third parties are used to simulate "attacks" on the system from the perspective of an outside threat in order to find backdoors or other weaknesses that are not readily apparent in the system.

5.6.8.1 VULNERABILITY MANAGEMENT

The most common security exploitations leverage known vulnerabilities. Vulnerability Management minimizes risk associated with known vulnerabilities by seeking to discover and remove the number of vulnerabilities in the company's business operations and infrastructure. This approach will be applied to known vulnerabilities in Smart Grid technologies prior to deployment and monitored throughout their lifecycle.

The Vulnerability Management Program tracks reporting and remediation of known vulnerabilities across multiple information resources by monitoring vendors which provide and support enterprise information and controls systems, a number of public and limited distribution vulnerability reporting lists, and tracking and reporting vulnerabilities discovered during internal testing activities. The program ensures systems maintain current, supported patches and upgrade levels.

Functions of the Vulnerability Management program include:

- Penetration Testing: Evaluating the security of a computer system or network by simulating attacks from a malicious source.

- Application Scans: Attempts to identify vulnerabilities in the application and/or web layers.
- Validation Scans: Attempts to identify vulnerabilities in the host operating systems, like Windows, Linux, UNIX, etc.
- Reports: Request results from a monthly scheduled scan or one of the above service requests.

Vulnerability Management activities also uses the company risk acceptance process. Under some circumstances it is necessary to document the acceptance of business risk resulting from a gap between the applicable security requirement(s) and the implemented security features and controls.

5.6.8.2 INCIDENT RESPONSE & RECOVERY

While the goal of the company's Information Security Program is to proactively avoid incidents which threaten to compromise company data, systems or related assets using proactive means, it also governs SDG&E's response to incidents. A disorganized reaction to an Information Security incident can be as damaging to the company as the incident itself. Therefore, it is important to follow a well-defined process in response, with clear coordination responsibilities. The following describes the Incident Response and Recovery process followed in the event of an Information Security incident which puts company assets at risk.

5.6.8.3 COMPUTER INCIDENT RESPONSE TEAM (CIRT)

The Computer Incident Response Team (CIRT) team is responsible for detecting, responding to, and assisting in the recovery from computer security incidents that impair the company's ability to:

- Generate, transmit or distribute energy;
- Conduct normal business operations;
- Operate in a secure computing environment;

- Threaten the privacy of customers.

5.6.8.4 INCIDENT RESPONSE PROCESS

The Incident Response process is initiated when the Security Operations Center (SOC), a 7x24 team dedicated to monitoring enterprise security, detects or receives a report of a security event. The team collects and evaluates the information in order to assess whether the event is an incident. If the event is an incident, the CIRT team, with appropriate predefined members based on the nature of the incident, is activated.

The CIRT Team manages the incident response, recovery and post-incident notification and reporting by:

- Performing a triage to determine the best course of action, gathering information on how to resolve the incident, how to contain the effects, and consult with the appropriate corporate management representative before actions are taken;
- Taking actions to halt and contain immediate damage due to an incident;
- Remediating the affected systems to "fix" the damage caused by an incident;
- Observing the assets behavior in order to gain information as to the nature of the incident, and potentially identify a larger issue;
- Determining whether or not the formal Forensics Process needs to be initiated, given the information about the incident available. If the Forensics Process is initiated, the results are reported back to the CIRT;
- Performing or requesting a Root Cause Analysis (RCA) to determine the basic reason for the incident, and suggest a course of action to prevent the incident from re-occurring;
- Determining the final actions and activities needed to return the company system and network to a "known secure state," and to prevent the incident from re-occurring; which may involve policy alteration, security training, component

upgrades, patch application, or other remediation actions. Specifically, the Risk Management process may (and likely will) be called from these final actions;

- Collecting, documenting and protecting all event and situation data in the Security Event repository;
- Reporting to appropriate parties about the Incident.

5.6.8.5 INCIDENT RECOVERY PROCESS

If there has been a service impact, the CIRT Team Lead activates and coordinates with the Service Restoration Team (SRT) to respond to the outage by restoring service, while addressing the potential need for Forensics data maintenance, and Root Cause Analysis to be performed after the incident.

5.6.8.6 NOTIFICATION AND REPORTING

Depending on the system or Information involved in an incident, as well as regulatory requirements, different internal and external organizations will need to be informed regarding the incident. These organizations potentially include, but are not limited to, FERC, NERC, the Commission, ES-ISAC, the DHS, the FBI, other law enforcement agencies, and impacted customers.

5.7 SDG&E'S PHYSICAL SECURITY PROGRAM

Utilities have long recognized physical security threats as significant. As SDG&E moves more assets of increasing value further out into the field, including information assets, existing physical security threats will be exacerbated and new ones introduced. Having physical access to an information asset increases the likelihood the asset can be exploited. The company's Physical Security Program recognizes that as more information assets move out of well-protected data centers and into the field, more robust and faster responding physical security controls must also be applied.

5.7.1 INVESTIGATIONS

Physical security investigative capabilities extend over a service territory covering much of Southern California and part of Mexico in order to support Smart Grid physical security.

5.7.2 SITE SECURITY REVIEWS AND VULNERABILITY ASSESSMENTS

Critical sites must be reviewed by corporate security representatives that have been trained in assessing physical security of facilities and properties for threats and vulnerabilities. Discovered vulnerabilities are prioritized and communicated to risk owners to make decisions about how to avoid, mitigate, transfer or accept these risks. Appropriate mitigations must be applied to reduce the risk to safety, as well as asset loss or damage.

5.7.3 PHYSICAL SECURITY MANAGEMENT

Physical security services must be effectively managed and expanded to incorporate Smart Grid infrastructure considerations. Such management services include:

- Guard Services - including management of employee or contractor guard forces;
- Technical Security Services - including facility clearing, and counter-surveillance measures; Video surveillance includes local and remote monitoring of activity at gates and other strategic locations. Live monitoring at guard stations and recorded video for incident investigation.
- Alarm Monitoring and Response

5.7.4 SECURITY COMPLIANCE

As with cyber security, facilities that support Smart Grid infrastructure and activities must comply with all legal, regulatory and company-driven standards and policies. Compliance must be easily verified and reportable.

Physical security capabilities for mission critical facilities are periodically reviewed by the DHS, NERC, and the Transportation Security Administration (TSA).

5.7.5 ACCESS ADMINISTRATION

Effective access administration includes facility access management capabilities, including the company's enterprise-wide badge access system. Employees, vendors, contractors are required to have photo ID/access badge displayed while on site. Access is in accordance with all applicable law and regulation, including to FERC requirements.

5.7.6 SECURITY AWARENESS AND TRAINING

Employee and third party awareness and training of physical security threats and vulnerabilities are a core part of the security program and incorporate relevant sabotage awareness, threat detection and reporting mechanisms.

5.7.7 THREAT MONITORING, GLOBAL EVENT NOTIFICATION AND ALERTS

Threat information sharing must be integrated and flow easily not only between company physical and cyber security programs but also between these programs and relevant law enforcement and intelligence agencies.

5.8 SDG&E RESPONSES TO COMMISSION QUESTIONS REGARDING PRIVACY

This section contains SDG&E's responses to the questions posed to the California Investor Owned Utilities by the Commission in Ordering Paragraph 10 of D.10-06-047 concerning the security of customer information.

5.8.1 INFORMATION COLLECTED VIA SMART METERS, PURPOSES, MINIMIZATION

What types of information about customers are or will be collected via the smart meters, and what are the purposes of the information collection? Could the information collection be minimized without failing to meet the specified purposes?

SDG&E's smart meters are capable of storing many types of energy related data. However, smart meters do not store customer data other than energy measurement data. SDG&E's smart meters are programmed to store energy measurement data that is required for billing. Additionally, SDG&E's smart meters collect different energy measurement data depending on the electric rate or tariff associated with the customer's account. Generally, SDG&E's smart meters collect register reads and interval reads for electric meters and register reads for gas meters. In addition to the energy measurement data SDG&E also collects information related to 'events' from the meter, such as a tamper alarm, and other information that allows the company to validate the accuracy of the data collected and transmitted back to SDG&E. In order to be assured of accurate billing information and ascertain the status of tampering, outages and other events, the data collected is necessary and cannot be minimized.

Below is a listing of the information being collected by SDG&E's smart meters by customer class. As stated, SDG&E's smart meters are capable of being programmed to collect many types of information; examples of these additional capabilities are included in Appendix 5.10.2.

Basic Residential

1. Delivered Register Read
2. Received Register Read
3. Total Register – Delivered plus Received
4. Delivered hourly intervals
5. Event information such as tamper alarms or outage information

Basic Commercial

1. Delivered Register Read
2. Received Register Read
3. Net Register – Delivered minus Received
4. Delivered 15 minute intervals
5. Event information such as tamper alarms or outage information

Advanced Residential & Commercial (e.g. co-generation, bi-directional)

1. Delivered Register Read
2. Received Register Read
3. Net Register – Delivered minus Received
4. Delivered 15 minute intervals
5. Received 15 minute intervals
6. Event information such as tamper alarms or outage information

Notes:

1. Delivered means energy delivered from utility to the customer.
2. Received means energy delivered from customer to the utility (e.g., from a roof-top solar installation).

5.8.2 EXPECTED DEVICES AND ASSOCIATED INFORMATION

Does SDG&E have or expect to have other types of devices, such as programmable communicating thermostats, which can collect information about customers? If so, what types of information are collected, and what are the purposes of the information collection? Could the information collection be minimized without interfering with the specified purposes?

SDG&E is piloting new technologies that enable devices inside the home, such as in-home displays, programmable communicating thermostats and other "smart" communicating devices, to be commissioned to the customer's smart meter (collectively, Home Area Network or HAN devices). These devices will present information, such as consumption or price, and will be capable of receiving signals controlling end-use devices based on established preferences set by SDG&E customers.

Information collected by these HAN devices is manufacturer and device dependent. SDG&E's smart meters are equipped with ZigBee transceivers and the ZigBee Smart Energy Profile (SEP). The ZigBee SEP protocol provides for customer acknowledgements, such as acknowledging that a message was received, or a choice to opt-out from a demand response event. Devices that use profiles other than ZigBee SEP may collect device state information, such as the current thermostat set point, mode (cooling or heating) and/or current temperature sensed by the thermostat. Certain end-use metering devices may collect interval consumption data of the end-use appliance. Other, more capable devices, may record all information input by the user similar to the capabilities of a personal computer (e.g., tablet computers used as in-home displays or ZigBee USB dongles that would use a customer's computer as the user interface for their HAN).

Minimizing information collection must be balanced with the information needed for a meaningful customer experience and realization of customer, utility and societal benefits. HAN devices exchange information with customers and the utility to enable

valued added services. Features that make devices desirable to customers may not be the same features that make them desirable for utilities. For example, utilities generally strive for operational, energy efficiency, demand response, and societal benefits. However, customers desire technologies that provide lower cost and greater choice, convenience, control, and comfort, as well as other tangible and intangible benefits. Customer requirements for information exchange may differ from that of utilities. Utilities may minimize device information collection to achieve utility operational and demand response benefits. However, minimizing data collection may result in lower adoption rates because some customers value greater amounts and frequency of information and customization of the experience. SDG&E intends for devices and systems to collect only the minimal information necessary to perform their functions and provide customers with features and options that provide value.

5.8.3 EXPECTED INFORMATION FROM SMART METERS AND HAN GATEWAY

What types of information, if any, does SDG&E plan to collect from the smart meter and Home Area Network gateway?

Details regarding smart meter data collection and capabilities are discussed in the response to question a, above. Regarding the Home Area Network gateway, this type of device serves as a communications conduit for securely commissioning various in home devices to the smart meter (such as a programmable communicating thermostat or an in-home display). The data collected includes Media Access Control (MAC) identification numbers, device type, serial number, and other similar data. The gateway maybe a conduit for data collected at the device level.

5.8.4 FREQUENCY OF INFORMATION COLLECTION FROM SMART METERS

How frequently will SDG&E take readings from the smart meter? Is this frequency subject to change? Will customers control this frequency?

As stated above, smart meters collect hourly or 15 minute interval data depending on the type of customer and the tariff associated with the customer account. In general and under normal circumstances, this data is transmitted to the utility twice each day. Energy usage intervals recorded at the meter can be changed, as can the frequency with which SDG&E collects this data from its Smart Meter system. The effective frequency of utility meter reads is based on the relevant tariffed rate being billed, information to be presented to customers, and system performance characteristics. SDG&E does not envision opening these systems' operational characteristics to customer control.

5.8.5 INFORMATION USAGE / PURPOSES

For each type of information identified above, for what purposes will the information be used? The purposes must be articulated with specificity, e.g., "targeted marketing" instead of "promoting energy efficiency."

As stated above, the information collected from SDG&E's smart meters and HAN system are used for billing and consumption information presentation purposes and to allow end-use devices to be commissioned to a particular customer's meter. Additionally, this information will be used to effectively manage the HAN system, allow verification of energy and capacity savings (demand response measurement and evaluation), possibly provide additional functionality to customers as the market continues its growth and more functionality is enabled by the Smart Grid, and possibly make customers aware of energy services they may find of value subject to affiliate compliance restrictions.

5.8.6 INFORMATION RETENTION PERIODS / PURPOSE OF RETENTION

For each type of information collected, for how long will the information be retained, and what is the purpose of the retention? Could the retention period be shortened without failing to meet the specified purpose?

Regarding data collected by home or premise area network devices, SDG&E is in the early stages of piloting systems to ascertain customer acceptance and satisfaction with these systems as well as to evaluate system, technology and device performance. Retention policies for the information associated with these systems have not been formally established, however SDG&E intends to retain this information for only as long as is necessary to meet these evaluation purposes. As these devices and systems become more widely deployed, data retention will also depend on the requirements associated with the verification of energy and capacity savings (demand response measurement and evaluation) and other demand response or price signal event acknowledgement purposes.

Regarding the data collected from SDG&E's smart meters, retention is driven by factors such as Electric Rule 18 (that states, in part, that if either a residential or nonresidential customer is found to have been overcharged due to billing error, the calculation of the amount of the overcharge for refund to the customer is for up to a period of three years), credit, meter revenue protection, load research, rate design, and system planning requirements. For credit purposes, the retention requirement for data is seven years which is tied to credit reporting requirements. This period of retention is also required by law if a customer disputes an item on their credit report, and thus, such retention is necessary. For meter revenue protection, legal requirements for reports and investigations are for a minimum of seven years plus the current year. However, for unauthorized use (which includes, but is not limited to, meter tampering, unauthorized connection or reconnection, theft or fraud) there is no limitation regarding the rebilling period and ideally, enough past information would be

available to re-bill for the entire period of the unauthorized use, which would benefit all other customers (these provisions are also found in Electric Rule 18).

In addition to the above requirements for customer / account specific meter data, there are also requirements to keep meter data for longer periods, however for these purposes the data does not necessarily need to be tied to a particular customer, but rather to general categories of customers (i.e.: residential / small commercial / large commercial or inland/desert/mountain/coastal climate zone or other customer groupings). These requirements are tied to such things as rate design and system planning. Additionally, load impact analysis associated with demand response or energy efficiency programs are required over periods extending up to 10 years as are price elasticity studies that require a substantial amount of pre and post rate treatment usage information (up to 10 years). This data is retained up to 15 years.

SDG&E's records retention policies evolve over time and with the deployment of the Smart Meter system, these policies are being reviewed in detail to determine necessary changes. The above noted requirements will be the drivers in determining updated retention requirements for the types of data discussed.

5.8.7 DATA SHARING AND ASSOCIATED ISSUES

(1) With whom does SDG&E share customer information and energy data currently?

SDG&E currently provides customers with access to their usage data via various online applications and is planning to provide additional channels in the future.

For large commercial and industrial (C&I) customers who currently have interval data meters with telecommunication (generally 200 kW or greater), usage data at the 15 minute interval is provided on-line via the kWickView application. The C&I customer accesses the kWickView application through SDG&Es website at www.sdge.com. The kWickView application has been available online to large C&I customers since 2001. In addition to energy usage data (kWh), kWickView provides customer specific monthly

demand (kW) for the billing month.

Residential customer access to SDG&E smart meter hourly consumption data is available via Google's PowerMeter gadget. SDG&E customers who choose to access their consumption data via Google's PowerMeter must register with SDG&E as a My Account customer and must provide explicit consent[35] for the transfer of their interval usage data to Google during the Google PowerMeter enrollment process.

SDG&E shares customer information and energy data with various third parties with whom it contracts for such purposes as on-line energy data presentment, credit checks, collection agencies, administration of demand response and energy efficiency programs, facilitation of meter installations, SDG&E brochure or other mailings, e-mail contacts concerning their gas or electric service, to facilitate on-line payment of bills, and administration of low income programs (such as California Alternate Rates for Energy or CARE) among other reasons. In cases when SDG&E does share customer data with a third party, contractual terms and conditions are included to protect such data and, if necessary, hold the third parties accountable if such data is not handled properly.

(2) With whom does SDG&E reasonably foresee sharing data in the future?

SDG&E plans to continue to offer a variety of on-line energy management tools to customers in the future so that customers can track their usage, identify the estimated bill-to-date, bill forecast data, projected month-end tiered rate, a rate calculator, and notifications to customers as they cross rate tiers.

SDG&E's future plans include mobile applications for customers and new experimental pilots on home energy management technologies that will likely involve third parties.

[35] The customer's consent may be made either by a manual signature or by electronic means; as set forth in SDG&E Advice Letter 2100-E, dated July 31, 2009.

SDG&E also envisions sharing certain kinds of data with third parties, such as aggregators, in accordance with its privacy policies and regulatory requirements in order to facilitate customer participation in such things as ancillary services market (leveraging their PEV or roof-top solar systems, for example) and perhaps other parties that the customer may designate (i.e., service providers).

In cases where data sharing is associated with secondary purposes (as defined in the CPUC proposed decision mailed May 6, 2011 adopting privacy rules), prior customer authorization will be obtained prior to gathering or sharing such data.

(3) What does SDG&E anticipate is or will be the purpose for which the third party will use the data?

Third parties such as aggregators may facilitate customer participation in such things as ancillary services markets (leveraging their PEV or roof-top solar systems, for example) and perhaps customers may designate release of data to other parties that will provide various energy management services, including rate analysis or appliance maintenance.

(4) What measures are or will be employed by SDG&E to protect the security and privacy of information shared with other entities?

SDG&E's internal policies regarding privacy protections and data exchange rules are based in part on the Commission's direction, federal and state statutes and Commission orders applicable to Commission-regulated companies. Numerous Commission decisions make clear that the California regulated utilities must keep sensitive customer information confidential (e.g., D. 01-07-032). Additionally, SDG&E places significant importance on protecting its customers' privacy as part a measure of good business practices for companies entrusted with such sensitive and confidential customer information.

Customer specific usage data as well as customer personally identifiable information (PII) are considered and treated by SDG&E as sensitive and confidential information.

PII includes any personal identification such as name, service/billing address, phone number, email address, and social security number. It also includes consumption information such as usage amounts and patterns and credit history such as records of customers' payment histories.

As the general rule, SDG&E does not release PII to a third party (e.g. data presentment or energy service providers) without obtaining the customer's prior explicit consent and authorization. There are, however, certain limited exceptions to the general rule. On limited occasion, SDG&E may be compelled or required by law to provide PII to law enforcement agencies upon receipt of a subpoena or other legally enforceable document demanding the information (e.g. a court order). SDG&E's policies pertaining to legal requests or demands for disclosures of PII data made pursuant to a subpoena or court order are discussed in more detail below. Depending upon the specific customer request received by SDG&E to release PII to a third party, SDG&E evaluates the specific type of customer usage data and intended purpose under the following general guidelines.

All requirements for data transfer, (e.g. Google's PowerMeter) is assessed against SDG&E's Information Security Requirements. Security requirements comport with efforts to adhere to a law, regulation, SDG&E security policy or best practice. Regulations and laws that apply to customer usage data transfer include:

- Sarbanes Oxley
- California Privacy Breach Notification Act
- HIPAA
- California Information Protection Laws
- Best practices which drive SDG&E requirements include:
- NIST 800/53 (Currently Rev 2; Rev 3 in development)
- NIST Interagency Report (IR) 7628
- BS-17799 (ISO 27002)

- Control Objectives for Information and Related Technology (COBIT)

SDG&E has several specific policies that govern proper access to customer energy usage data, such as:

- Password Policies
- Acceptable Use Policies
- Service Account Policies

Each of SDG&E security requirements are the result of and can be traced to a policy, law, regulation and/or best practices. Because of changes to regulations and laws over time, SDG&E reviews policies governing data security and privacy protection, at a minimum, on an annual basis.

Although the Smart Grid decision does not explicitly request that utilities address consumer protection issues that may arise as a result of third party energy management and information service providers, SDG&E believes statewide certification of third parties may be prudent to provide minimum protection and oversight of third parties. The Commission currently certifies energy service providers (ESPs) that provide Direct Access services to customers. A similar process could potentially be used to certify third parties requesting access to customer data.

The proposed decision of the Commission mailed on May 6 regarding privacy rules indicates that the Commission may not implement such a certification process for third parties[36]. If this direction is adopted, SDG&E will continue to work with the Commission on a legally acceptable process (due process) to cease transfer of customer data to bad actors.

[36] Finding of Fact 58 of the PD states "Because of the privacy protections adopted in this decision, because a residential customer may withdraw access to his or her consumption data at any time, and because the Commission can find a third party ineligible to receive data either via tariff or by refusing to interconnect a device that automatically transfers usage data to the third party, it is not necessary to create a registration process to certify third parties as eligible to receive usage data."

Additionally, for SDG&E contracted third parties, the legally binding contractual terms and conditions will protect customer information. SDG&E's standard confidentiality language includes the following provisions designed to protect customers' information:

- SDG&E uses a broad definition of "Confidential Information" to protect a wide range of information related to customers;
- SDG&E limits vendors' use of such Confidential Information to be solely for purposes of performing services under its agreements (i.e., vendors cannot use Confidential Information for their own benefit or commercial purposes);
- SDG&E requires vendors to use reasonable security procedures and practices to protect the Confidential Information from unauthorized access, destruction, use, modification or disclosure;
- SDG&E requires vendors to deliver or destroy any Confidential Information upon request; and
- SDG&E now specifies that its confidentiality provisions related to customer Confidential Information remain in effect perpetually.

(5) What limitations and restrictions will SDG&E place on third party use and retention of data and on downstream sharing?

Non-disclosure agreements (NDAs) are required for all consultants or contractors retained by SDG&E that are provided access to SDG&E customer data. The NDA provides contractual protection from unauthorized use or release of customer energy usage data or PII.

Each vendor is required to ensure each of its agents, representatives, subcontractors and suppliers become familiar with, and abide by, the customer confidentiality provisions in SDG&E's agreements as more fully described in the response to question 5.8.7 (4), above. Generally speaking, these customer confidentiality provisions prohibit the use or sharing of customers' confidential information for any purpose other than performing services for the utility under its agreements. Additionally, these provisions

include requirements to protect customer information using reasonable security measures and allow SDG&E to seek the return or destruction of any confidential information.

(6) How will SDG&E enforce those limitations and restrictions?

SDG&E has several options to enforce the customer confidentiality provisions in its agreements. In the event of a breach or a threatened breach of the customer confidentiality provisions of an SDG&E contract with a third party with whom it has shared data, SDG&E can generally:

- Obtain injunctive relief preventing a breach of customers' confidential information;
- Request the return or destruction of all or any part of customers' confidential information; or
- Seek monetary damages and other legal and equitable remedies.

5.8.8 AUDIT AND SECURITY PRACTICES

What measures are or will be employed by SDG&E to protect the security of customer information?

SDG&E has designated a Chief Privacy Officer whose responsibility it is to ensure the privacy of customer information that is in the custody of the utility.

In addition, SDG&E employs a robust information security program that focuses on the three core competencies that operate together to protect the security of customer information: Governance, Engineering and Operations.

The Security Governance organization is tasked with company security policy and policy compliance, which includes the drafting and maintenance of policy artifacts, and assurance that the company is in compliance with all required legal and regulatory cyber security requirements; security awareness, which ensures every employee understands

and executes their role in protecting company information; security strategy and architecture, which oversees the future direction of security controls across the company; and its security program office, which leads projects that implement new security controls. The Governance organization also maintains security contractual language that is used during negotiations with third parties to ensure that if the relationship calls for the sharing of company information, that the information is adequately protected.

The Security Engineering organization is responsible for developing and maintaining company security standards and requirements, and ensures that every new project adheres to such standards and requirements.

Finally, SDG&E's Security Operations organization is responsible for monitoring company networks and systems for potential cyber threats and vulnerabilities, ensuring that vulnerabilities are quickly remediated, and if threats materialize, they are contained quickly so the damage caused is minimized.

Has the utility audited or will it audit its security and privacy practices, both internally and by independent outside entities? If so, how often will there be audits? What are the audit results to date, if any?

As a supplement to system owner driven control processes, Sempra Energy's Audit Services department performs risk-based audits based on an annual audit plan. Confidentiality of customer data and security practices are considered when developing annual audit plans. The frequency of internal audits of customer information and privacy controls are dependent on the outcome of the annual risk assessment process. On occasion, the company also engages independent outside entities to perform targeted assessments of SDG&E security practices and controls.

The company considers audit reports and the associated findings, if any, to be confidential. The company's security and privacy practices protect confidential information from public disclosure.

5.9 CONCLUSION

The Commission and the public are concerned about the potential physical and cyber security risks posed by Smart Grid. It is incumbent on all of Smart Grid participants, including utilities, regulators, service providers and consumers, to do their part to ensure that the system all participants rely on to deliver safe and reliable energy to our homes and businesses is resistant to threats and resilient to disaster.

SDG&E believes that if Smart Grid is implemented according to its security strategy, its advantages to customers and the communities it serves will far outweigh its potential risk.

5.10 APPENDIX

5.10.1 SAMPLE MATRIX OF UNIFIED SECURITY CONTROLS FRAMEWORK TO VARIOUS SECURITY GUIDELINES

The sample Common or "Unified" control framework below is provided for illustrative purposes only. It is not intended to show SDG&E's entire library of security controls and control activities, nor does it represent the complete list of standards and regulatory requirements SDG&E is obligated to comply with.

Table 5-2: Sample Matrix of Unified Security Controls Framework to Various Security Guidelines

Sample Common or "Unified" Control Activity	ISO 17799 (2000)	NERC CIP	COBIT	NIST 800-53	AMI Security Profile	DHS Catalog of Control Systems	DHS Procurement Language	"..."
Access to administration utilities shall be strictly controlled and maintained separately from application functions.	9.5.5.B			AC-3(1)	DHS-2.8.3.1	2.8.3.1		x
Access to administration utilities shall be limited to the minimum practical number of authorized users.	9.5.5.C							x
Activities performed using administration utilities shall be logged.	9.5.5.F				DHS-2.16.2.1	2.16.2.1	4.4	x
Persons and processes that have access to administration utilities shall be documented.	9.5.5.G				DHS-2.10.8.1	2.10.8.1		x
Unnecessary utilities and system software shall be removed from Sempra information assets.	9.5.5.H			CM-7 (1)	DHS-2.15.7.3	2.14.3.2	2.1.3	x
Sensitive information shall not be transmitted to output devices (e.g. printers, web sites, unencrypted email) where they cannot be protected in accordance with their sensitivity.	9.6.1.D		DS13.4	PE-5				x
Information assets shall be monitored to detect deviation from access control policies.	9.7	CIP-007 R6, R6.1, R6.2	PO8.6, DS3.5, DS5.5, DS13.3	CA-7				x
Users and automated processes shall be identified by unique User IDs and authenticated by cryptographic mechanisms or passwords compliant with the Sempra Password Standard.	9.2.1.A		DS5.3	IA-1 IA-2(1) IA-5	DHS-2.15.16.3	2.15.5.2 2.15.16.2	4.3.3	x
"..."	x	x	x	x	x	x	x	x

5.10.2 LISTING OF POSSIBLE SMART METER DATA ELEMENTS

The following table, Table 5-3, lists the data elements available on smart meters.

Table 5-3: Smart Meter Data Elements

Examples of SDG&E Smart Meter Capabilities

Selected Categories / Elements that can be recorded (Commercial and/or Residential meters)

Measurements
Energy Reading
Forward Energy Kwh
Reverse Energy Kwh
Net Energy (Fwd + Rev)
Net Energy (Fwd - Rev)
Demand KW
Demand KVAR
Demand KVA
TOU Data
Critical Peak Period Data (TOU)
Date
Time
Meter Status & Errors
RAM bit error
Hard EEPROM error
Configuration error
Clock Error
Low battery
Load Profile Overflow
Meter Alarms and status
Service Condition Status
Power failure
Reverse power
Out of Socket alarm

Meter Info
voltage
max amps (class)
Hardware Version
Firmware Version
Comm Info
Firmware Version
AMI SN

Module Status & Erros
RAM ROM fail
History overflow
Remote Communications Inactive
Controls
Demand Threshold Alert
Set and update time
reset error codes
Reset momentary outage counts
Power Quality - Voltage Measurements
Max Voltage
Min Voltage
Current Voltage (Inst)
Power Quality - Current Measurements
Instantaneous RMS current A
Instantaneous RMS current B
Instanteneous RMS current C
Status / Alarms
Meter Tamper
Outages
Momentary date and time
Outage date & time
Restoral date & time
Security
Invalid Password
Radio Performance
Transmit Power

5.11 REFERENCE MATERIALS

- *NISTIR 7628: Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements*, http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf
- *NISTIR 7628: Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid,* http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf
- *NISTIR 7628: Guidelines for Smart Grid Cyber Security: Vol. 3, Supportive Analysis and References*, http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf
- *Security Profile for Advanced Metering Infrastructure, v 1.0, Advanced Security Acceleration Project – Smart Grid*, December 10, 2009
- *Catalog of Control Systems Security: Recommendations for Standards Developers*, U.S. DHS, National Cyber Security Division, September 2009
- *DHS Cyber Security Procurement Language for Control Systems*
- *SGIP Smart Grid Conceptual Model, Version 1,* April 2010
- *NIST High-Impact, Low-Frequency Event Risk to the North American Bulk Power System*, http://www.nerc.com/files/HILF.pdf
- *Privacy by Design: Achieving the Gold Standard in Data Protection for the Smart Grid*
- *Privacy by Design: Seven Foundational Principles,* http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf
- *SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation*