

SCE response to questions for the DHS Subcommittee for Cybersecurity, Emerging Threats and Science and Technology on July 21st

Q: How much of the total cost of its metering infrastructure does SCE expect to recoup from rate cases?

A: SCE's smart meter program is authorized for full rate recovery by the California Public Utilities Commission.

Q: Are SCE's assets hardened against an intentional or unintentional electromagnetic pulse? If so, how did SCE go about mitigating this threat? How much did implementing protective measures cost? Was SCE able to recoup these costs in a rate case?

A: SCE understands the disruption potential of electromagnetic pulse (EMP) and other threats that pose risks to system availability. These threats are taken into account as part of our system design. The risk of the SCE assets being affected by EMP is a function of the probability, size, and nature of an EMP threat. As such, SCE's risk-adaptive process accounts for this and other threats through our system availability, disaster recovery and business continuity designs.

Q: Please describe how SCE implemented mitigations to the Aurora vulnerability.

A: In response to the Aurora Vulnerability, SCE first performed a detailed assessment of the system to identify and mitigate the associated vulnerabilities across our service territory in alignment with NERC recommendations. Additionally, SCE refined planning, engineering, procurement, security and compliance policies to support NERC CIP standards.

Q: What would industry like to see from government in terms of an alert and warning system about an impending cyber attack? Does this early warning system exist today?

A: We believe the government has an important role to play in the case of impending security events. This role should be played in the broader context of a well-defined structure as articulated in SCE's white paper "A Lifecycle Framework for Self-sustaining Implementation of Smart Grid Interoperability and Cyber Security Standards" which is attached to this response. Early warning processes in use today include US-CERT, the Electric Sector-ISAC (ES-ISAC) managed through NERC, as well as the DHS Daily Open Source Infrastructure Report. All existing early warning processes would benefit from participating in a broader self-sustaining, framework that includes the mechanisms for all stakeholders including policymakers, vendors, utilities and incident response teams to take actions so the overall electric infrastructure becomes increasingly secure.

Q: What is the current role of the Federal government be in defending against nation state-level cyber or physical attacks against electric facilities? What should the role of the Federal government be?

A: We believe the role of the federal government should be to work with industry to align collaborative efforts on policy, standards development, product development and procurement actions

to create the self-sustaining Smart Grid market as outlined in the attached white paper “A Lifecycle Framework for Self-sustaining Implementation of Smart Grid Interoperability and Cyber Security Standards” . A successfully operating, self-sustaining market is defined by public policy supported by standards that are rapidly adopted by product vendors seeking certification, and driven by utility procurements buying products certified to those standards. The effect in the market place is that product vendors are incented to compete against each other to create Smart Grid solutions that are increasingly interoperable and secure.

Q: Does SCE use the Energy ISAC today? Does SCE believe that the Energy ISAC is effective in producing timely and relevant analysis and warnings for the industry? If not, what measures can be undertaken to improve this capability?

A: Yes, SCE utilizes the Electric Sector-ISAC (ES-ISAC), managed through NERC, for warnings applicable to the electric sector. The ES-ISAC, notifications are supplemented by US-CERT, as a source for our Anti-vulnerability Emergency Response Team, a 24x7 group of SCE subject matter experts tasked with vulnerability and incident response.

We do believe the ES-ISAC represents an effective mechanism for timely and relevant analysis and warnings for the industry. ES-ISAC participation in the broader industry lifecycle framework, as stated in the attached white paper, would improve communication on security events and known vulnerabilities across a broad set of industry stakeholders.

Q: What are the key aspects of any piece of legislation that seeks to secure the electric grid from cyber and physical attack?

A: Legislation seeking to secure the electric grid should consider the ability to facilitate the standards-driven process which motivates the market to produce and adopt increasingly secure and interoperable products.

Q: Are industry-written security standards appropriate to protect assets as critical to national security as the electric system? If so, why? If not, should a Federal entity write the standards?

A: Yes, SCE believes a public/private partnership is the most effective way to develop cybersecurity specifications and standards. An example is the current effort between the industry, NIST and the Department of Energy, known as ASAP-SG, the goal of which is to organize and articulate Smart Grid cybersecurity standards by leveraging an existing set of standards will help provide the guidance necessary for vendors to develop secure product; certification labs to certify secure product; and utility companies the ability to confidently procure and implement secure products.

SCE has published three papers on the topic of security and standards please see:

<http://www.sce.com/PowerandEnvironment/smartgrid/>