POTENTIAL QUESTIONS FOR SUBSTATION SECURITY PANEL

1. Please introduce yourself, give a little background on yourself, and explain your organization's involvement in substation or grid security issues.
2. What is the current state of the threat environment with respect to electric utility infrastructure, important to the State of California? What do you see as the main concerns? Can you rank the risk in your opinion –Generation? Transmission? Substation? Distribution? Other (Communication infrastructure, fuel supply, etc)?
3. Aside from the Metcalf incident, are you aware of any major similar physical security incidents occurring in the United States in the last 20 years. Please discuss those events.
4. Please discuss your opinion of the relative importance of cyber or information security verses pure physical security. Is it possible to completely separate the two? Why or why not?
5. Where do you believe physical or cyber threats to generation fits into the hierarchy of risk? Is this something which needs to be addressed separately?
6. What are current best practice methods of mitigating physical security risk for the electric system, in particular substations but also lines and external structures. Please give some examples.
7. Do you have any issues with the current NERC proposed standard as written? If such shortcomings exist, would this be a place for state regulation, even at the bulk power level?
8. Knowing that 100% mitigation is not possible, how much of the potential risk (e.g., economic, environmental, public safety) is likely to be mitigated by the implementation of NERC CIP 014?
9. With most of the catastrophic or larger-scale/longer-term issues potentially being addressed at the federal level, what might be some of the benefits of taking measures on lower-level assets and do you think that they would justify the costs? Is a graded approach advisable and possible?
10. **Distribution System Flexibility** - Distribution networks are designed and built with significant operational flexibility that provides an inherent resiliency to disturbances. This includes higher availability of alternate paths for power, the capability to transfer load within the distribution network and more readily available spare equipment for emergent needs. What in the panel's view would be an appropriate method to identify perceived weakness in the current structure? Furthermore, why are current levels considered insufficient?
11. **Distribution Equipment Availability** - Spare equipment for distribution is readily available. Units are stored in multiple locations across utility service territories and procuring additional equipment can be done quickly due to relatively short lead times. What vulnerability does the panel believe exist from the perspective of availability of replacement equipment? Are there some best practices for management of spares for a distribution network?
12. Do you see vandalism, as opposed to intentional terrorism, as a significant security risk to the electric distribution system? Should this be addressed separately as part of any physical security regulations?
13. The attention on the Metcalf incident and the NERC standards both focus on critical, FERC-jurisdictional substations. This focus is consistent with a National Research Council study, which finds that failure of equipment at substations can lead to widespread, sustained outages. That study, however, recommended not only reducing the vulnerability of critical infrastructure, but also made recommendations to utilities, law enforcement, state legislatures, and public utility commissions regarding emergency preparedness and the implementation of "smart" infrastructure.

a. *In what ways is a utility's preparation for an outage caused by a natural disaster sufficient to prepare for an outage caused by a maleficent actor? In what ways might that preparation be insufficient for an outage caused by a maleficent actor?*
b. *What should the Commission be doing to make the power delivery system less vulnerable to security threats, reduce the consequences of successful security breaches, improve the speed of power restoration, and make critical services less vulnerable when power has been disrupted?*
c. *What resources does the Commission have to determine whether a utility's security actions are sufficient or insufficient? Can the Commission play a role in overseeing utility security plans or setting security standards until it has the capability of determining the quality of a utility security program?*
d. *How should the Commission coordinate with OES, law enforcement, municipal utilities, and others?*

14. The Commission's (including ORA's) access to utility information is almost unfettered (PU Code 314: "The commission, each commissioner, and each officer and person employed by the commission may, at any time, inspect the accounts, books, papers, and documents of any public utility). This access is in large part transferred through discovery rights to intervenors who sign non-disclosure agreements (NDAs) in general rate cases.

a. *Are the Commission's procedures and practices appropriate for handling sensitive security information (SSI)?*
b. *Does the Commission have the procedures and information technology to protect such information?*
c. *How much SSI does the Commission need to fulfill its regulatory responsibilities, and should it limit the information it asks of the utilities?*
d. *What standards or guidelines are available to the Commission in deciding what type and level of detail of information is in the public interest to release publically, and what information is in the public interest to keep confidential? (i.e. 49 CFR 15, etc.) Is GO 66-C sufficient?*