The California Military Department

California Military Department
Computer Network Defense Team
9800 Goethe Road, MS # 4
Sacramento, CA 95827
(916) 369-5003

June 12, 2014

With regards to the two complex, multi-part questions posed, the responses are provided from a purely Cyber Security perspective, not that of a physical security one which is more appropriate for some subparts.

1. 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.

Subpart 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?

Response: From a cyber risk perspective, a cyber attack that results in a kinetic manifestation (cyber event resulting in real-world physical damage) of a critical component would results in a similar response. For example, DOE's Operation Aurora in 2007 addressed a cyber attack on a large power generator, causing a catastrophic failure. This cyber to kinetic result had a consequence management step of replacement of the generator. This portion of the incident response plan is not dissimilar to that of a natural disasters (or terrorist event) where permanent damage to the same device could result. What is different between these events (natural, manmade, and cyber incident) are the pre-incident security mitigation measures. So, while the consequence response steps are not dissimilar, the pre-incident measures, monitoring, detection, and protections are vastly diverse.

Subpart 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?

Response: From a cyber perspective, information systems and communication protections are expensive and complex; you can't protect everything so you protect the critical componentsand communications interconnects used for command and control A proposed method to accomplish this would be to establish minimum baseline metrics in which to measure cyber security compliance that would be universally implemented by all providers with the CPUC regulatory scope. These metrics would consider the following factors:

1. Data Classification: Cyber security controls are typicallyallocated based on a weighted or "Classification" of information or resource methodology. Less critical systems and

communications require less governance controls because the organization can tolerate higher levels of interruption of service prior to a catastrophic failure event occurrence. By standardizing a weighted classification based on components, data, and communications systems criticality, logical and physical protections can be applied, providing the highest ROIfrom a protective and capital investment perspective. I would suggest the commission review the below relevant references in this regard:

- FIPS 199 which addresses the concept from a high level.
- NIST 800-60 series (Vol 1 & 2)
- Sandia Report SAND2007-3888P, July 2007, Security Framework for Control System Data Classification and Protection
- NERC Standards CIP-002-3 through CIP-009-3. Note: I would caution the counsel that these standards are open to broad provider interpretation and as such would be difficult to define a one size fits all success metric as written.

2. Application of an Industry Governance standard for metrics measurement. There are several models that are applicable. In specialized industry verticals such as ICS, NIST 80082 provides a unique sector specific control management perspective. This would be an excellent baseline to consider.

3. An implementation plan, timeline, and reporting standard for providers to disclose their compliance metrics. In this matter, the Department of Homeland Security hasseveral programs. One of interest to the commission may be the Cyber Resilience Review (CRR). The POC for more information on this program is Mr. Deron McElroy, (415) 484-9222. The plan should address any legislative or regulatory requirements to comply with the standard (which could be a phased implementation to reduce complexity and spread costs over a wider time horizon)and the necessity for the reporting metrics. They metrics would provide the commission a method to evaluate the larger risks to the interconnected SCADA systems and their potential citizen impacts during an incident.

Subpart c: What resources does the Commission have to determine whether a utility's security actions are sufficient or insufficient?

Response: Please see response for Question Subpart B.

Subpart d: 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?

Response: Please see response for Question Subpart B.

Subpart e: How should the Commission coordinate with OES, law enforcement, municipal utilities, and others?

Response: Once the commission determines the metrics for the "Way Forward", the engagement of consequence management partners from OES, LEO's, Utility Districts, and Federal Law enforcement would provide the commission an excellent partner working group to further refine and develop communication methods for incidents, response plans, anddevelopment of both Table Top Exercises (TTX) and Incident Response Exercises designed to test, refine, and mitigation and strengthen response measures. CalOES and DHS would be excellent partners to work these plans for the commission.

2. 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.

Subpart a: Are the Commission's procedures and practices appropriate for handling sensitive security information (SSI)?

Response: Referring to response Question 1, subpart b, subsection1, once data is classified, protective measures regarding the retention, sharing, and storage of the Sensitive Information (SI) would be better understood. Once better understood, this question could be better addressed. One consideration the commission must consider the aggregation of SI can cause the repository to achieve a higher level of classification and therefore require additional protections.

Example: Vulnerabilities of Utility A are hypothetically rated as "Sensitive– Not for Public Disclosure", FIPS Level Moderate, encrypted and maintained on the Utilities network. This type of data is referred to by DHS as Protected Critical Infrastructure Information (PCII). If Utilities A, B, C, & D were to provide this data to the commission, the disclosure could be used to determine a common vulnerability across all utilities, representing a higher level of risk to the overall grid. This enhanced risk and increased exploitation opportunity for bad actors would necessitate a higher classification level and protective measures. This could necessitate protective measures such as air-gap or off-line processing requirements to ensure the protections of the information. The commission should consider the impacts of becoming a collective repository and the impacts should data breach of PCII data occur.

Subpart b: Does the Commission have the procedures and information technology to protect such information?

Response: Once a classification metric is established, a Cyber Health Assessment could be conducted by the California Military Department Computer Network Defense team (CND) to assist the commission in understanding their current cyber risk exposure. Once assessed, that question could be better addressed.

Subpart c: How much SSI does the Commission need to fulfill its regulatory responsibilities, and should it limit the information it asks of the utilities?

Response: This is a valid question. Does the commission need to generalized risk ratings or the detailed information? This would be dependent on the metrics established and the supportive regulatory / legislative requirements as addressed in Question 1, Subpart b, response 3.

Subpart 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?

Response: If you follow the generalized guidelines adopted by DHS for Protected critical infrastructure information (PCII), then this data would be restricted from public disclosure. Alternatively, the commission could develop a disassociated metrics report card per utility and

publish this. This would be permissible in theory only if doing so did not expose specific areas to target for vulnerability by bad actors for utilities.

I hope these responses provide you the information you are seeking. If the commission requires further clarification or has follow on questions, I will make myself available via audio conference line to provide whatever assistance possible. I can be reached directly at (916) 369-5069.

Ken Foster
Cyber Operations Manager
Computer Network Defense Team (CND-T)
CA Military Department