

**COMMISSIONERS**  
BOB STUMP - Chairman  
GARY PIERCE  
BRENDA BURNS  
BOB BURNS  
SUSAN BITTER SMITH



**ARIZONA CORPORATION COMMISSION**

Bob Stump  
Chairman

Direct Line: (602) 542-3935  
Fax: (602) 542-0752  
E-mail: bstump@azcc.gov

March 3, 2014

Barbara Lockwood  
General Manager, Regulatory Affairs and Compliance  
Arizona Public Service Company  
P.O. Box 53999  
Mail Station 9659  
Phoenix, Arizona 85072

M. Jo Smith  
Senior Director, Regulatory Services  
TEP and UniSource Energy Services  
88 E. Broadway  
Tucson, Arizona 85701

Robert R. Taylor  
Regulatory Policy and Public Involvement  
Salt River Project  
P.O. Box 52025  
M/SPAB221  
Phoenix, Arizona 85072-2025

John Wallace  
Director, Strategic & Regulatory Affairs  
Grand Canyon State Electric Cooperative Association, Inc.  
2210 S. Priest Drive  
Tempe, Arizona 85282

Dear Ms. Lockwood, Ms. Smith, Mr. Taylor and Mr. Wallace:

Recent attacks on our nation's power infrastructure are a clarion call for regulators and utilities.

Last year's attack on the Metcalf power station, in San Jose, California, may be a harbinger of more successful – and serious – attacks. Threats will surely increase in sophistication and frequency, and it behooves us to gain a more complete picture of Arizona utilities' efforts to protect its infrastructure – both cyber and physical – from devastation.

As we all know, snipers opened fire for nearly 20 minutes on an electrical substation, in California, surgically disabling 17 large transformers which help provide power to Silicon Valley. The perpetrators have yet to be apprehended.

We can only pray that Arizona never suffers such an attack. And yet we must be vigilant and we must be prepared. To that end, we would appreciate your answers to the following questions. We thank the National Association of Regulatory Commissioners for their help in designing appropriate questions to ask utilities on this topic.

1. Does your cybersecurity plan contain both cyber and physical security components, or does your physical security plan identify critical cyber assets?
2. Are interdependent service providers (for example, fuel suppliers, telecommunications providers, meter data processors) included in risk assessments?
3. Does your cybersecurity plan include alternative methods for meeting critical functional responsibilities in the absence of an IT or communication technology?
4. Has your company conducted a cybersecurity evaluation of key assets in concert with the National Cyber Security Division of the Department of Homeland Security? Has your company had contact with the National Cyber Security Division of DHS or other elements of DHS that may be helpful in this area?
5. What collaborative organizations or efforts has your company interacted with or become involved with to improve its cybersecurity posture (such as NESCO, NESCOR, Fusion Centers, Infragard, US-CERT, ICS-CERT, ES-ISAC, SANS, the Cross-Sector Cyber Security Working Group of the National Sector Partnership, etc.?).
6. Compliance as a floor, not a ceiling: Are there beyond-compliance activities? Given that there are very little or no cybersecurity standards specified at this point by state regulatory authorities with regard to the distribution portion of the electrical grid, what are you doing to get in front of this?
7. Are there third-party providers of services whose cybersecurity controls are beyond the ability of your organization to monitor, understand, or assure? Has your organization explored whether these may create cybersecurity vulnerabilities to your operations?
8. Does your organization perform vulnerability assessment activities as part of the acquisition cycle for products in each of the following areas: cybersecurity, SCADA, smart grid, internet connectivity and Web site hosting?
9. Has the company managed cybersecurity in the replacement and upgrade cycle of its networked equipment?
10. What personnel background checking is performed for those with access to key cyber components? Are vendors and other third parties that have access to key cyber systems screened?

11. For the most critical systems, are multiple operators required to implement changes that risk consequential events? Is a Change Management process in place, especially in regard to systems which could present a risk to electrical reliability?
12. Has cybersecurity been identified in the physical security plans for the assets, reflecting planning for a blended cyber/physical attack?
13. What reporting occurs in the event of an attempted cybersecurity breach, successful or not? To whom is this report provided (internal and external)? What reporting is required and what is courtesy reporting?

Due to the serious nature of this issue, we encourage the companies to elaborate on any ongoing additional efforts they can discuss publicly without compromising security/privacy.

Thank you for your help in this matter.

Sincerely,



Bob Stump  
Chairman  
Member, NARUC Committee on Critical  
Infrastructure  
NARUC Board of Directors



Robert L. Burns  
Commissioner