



Memorandum

Date: August 30, 2014
To: Chris Johns, President
From: Stephanie Douglas, Senior Director, Corporate Security
Subject: Recommendations for Security

PREDICATION

The 2013 Metcalf attack dramatically demonstrated significant weaknesses in the company's security posture and procedures at critical facilities. Since then, CSD has worked hard along with Electric Operations to improve security through a number of significant initiatives at substations. These efforts, however, have been undertaken within a CSD framework and resource structure which has remained unchanged from before the attack on Metcalf. Due to the existing structure and limited authority of CSD, little has changed relative to CSD's abilities to make significant and intended security improvements. These improvements continue to be slow, piecemeal and uncertain. **Recent events revealed the continued inadequacy of this approach.**

In the late night hours of August 26th and early morning hours of August 27, 2014, unidentified intruders entered the General Construction Yard and then the substation at Metcalf. Despite triggering certain alarms and the presence of two onsite security officers, the intruders accomplished thefts of several substantial pieces of equipment. As a result, a review of the responsiveness of the Fairfield Security Control Center and the onsite security officer vendor in response to this incident is underway.

RECOMMENDATIONS

Senior Director, Stephanie Douglas recommends the following to assess the capabilities and the capacity of Corporate Security Department (CSD) and to also empower it to function with authority.

1) Establish independent funding mechanism for CSD – currently CSD has no ability to pay for any security enhancement or most of the maintenance of security assets; instead each item is a discussion and negotiation with the relevant Line of Business (LOB). Decisions to either fund or deny funding are made at certain levels which do not come to the attention of senior management. Therefore, we risk not knowing about security issues and having gaps exist for some time before the issue is resolved.

This impacts not only how security assets are funded but it directly hinders any authority CSD has as a security element in the company. It also consumes a great deal of personnel resources and is not appropriately tracked. The CSD budget is currently funded at a little over \$4M with over 90% of it spent on personnel resources. This gives little flexibility to do anything else.

2) Establish a Senior Executive directly responsible for security - currently CSD reports to a VP level in the company. The current reporting structure does not have resourcing powers to include financial or personnel resourcing. This hinders CSD's ability to surge resources if needed and again places it in a discretionary role to other LOBs. Many utilities demonstrate the importance of security by elevating this role. It also ensures a more comprehensive understanding of the realities of the security landscape by all senior officers.



Memorandum

3) Appropriately staff CSD – currently CSD is staffed with a total of 26 FTE. Seven of these resources are designated for physical security work, with one designated supervisor and one designated manager. Electric Operations has approximately 900 substations alone. CSD also is accountable for providing physical security to other LOBs, to include Gas Operations, Customer Service and the General Office. CSD also has the responsibility of doing all internal criminal and most code of conduct cases, access management functions, NERC CIP compliance relative to physical security, and has the Executive Protection Program and Workplace Violence Program as well. ***To date, there has been no increase in the CSD budget or its staffing since prior to the April 2013 Metcalf attack with the exception of one Physical Security Specialist and an Investigations Manager.***

The anticipated growth of the responsibilities and the demands for physical security are already outpacing any potential for personnel growth given the flat budget. It is currently anticipated that the CSD labor costs for 2014 will exceed those budgeted. In the current “flat” budget environment, CSD cannot increase staffing unless funded by another LOB. For 2015, there is a significant TO 16 ask which may enable CSD to enhance personnel since so much of its work is in support of Transmission Operations. However, there is already confusion on what this money will cover as Electric now believes CSD should include any maintenance of equipment in this funding.

In addition to the above, it is recommended two outside reviews be done expeditiously. These reviews should be conducted by third party experts with significant security experience. They should be aggressive and specific and are:

1) CSD Performance Review: Given the events of the last week, the performance of CSD and its vendors should be questioned. As a result, I recommend a thorough third party review of CSD. *In reality, this should have happened immediately after the events of April 2013 but should certainly happen now.* Items to be covered would include but should not be limited to:

- Roles and Responsibilities to include Reporting Structure
- Management and Personnel Performance
- Resources/Scope of Duties
- Training
- Existing Management Tools
- Records Management
- Internal and External Liaison
- Facilities
- Budget
- Planning
- Metrics

Estimated Time Required: 90 days

Estimated Cost: \$500,000

2) Technical Review: In reality, CSD cannot firmly account for what security assets are in place other than by a manual and highly unreliable mechanism, The company’s existing security infrastructure is an assortment of technologies, many of them outdated. They have been cobbled together over the past 25 years and I would consider them to be in a “fail” mode. For instance, during the weekend of August 30, 2014, CSD lost all ability to see alarms at any of the approximate 100 Customer Service Centers. Thankfully, the video cameras were still functioning which gave Fairfield Security Control Center (FSCC) an opportunity to scroll through



Memorandum

these cameras to see if anything was amiss. FSCC also contacted the appropriate Directors to make them aware and arranged for law enforcement notifications as well. However, because of the volumes of video traffic across the limited network, the process is overly burdensome and time consuming. It also distracts from the operators primary duty of appropriately responding to active alarms. While both IT and the vendor have been working on this for 2 days now, the system is still not functioning as of 4:58PM.

The Technical Review should include but not be limited to:

An inventory of existing security equipment and details as to its location
Creation of an asset management and maintenance tracking tool (with IT)
Identification of dated and failing equipment and make recommendations for replacement
Working off what already exists, specifically recommend and provide detail plans for a higher functioning security control center including a resource plan, training, space, and technology OR provide options of a third party management of control center functions
Prioritize work over a five year period
Provide estimates for each

Estimated Time Required: 120-180 days

Estimated Cost: \$1M

SUMMARY

The physical security infrastructure of PGE has plenty of work to be done. While we have made progress in identifying some of our significant gaps and are making headway, in reality PGE is years away from a healthy and robust physical security posture. These are just a few things to be considered in addressing the gaps we currently face.

I know that some of these recommendations will be met with some hesitation. I am open to any discussion, ideas or suggestions but I firmly believe that without these basics, CSD will remain an entity which is unable to meet the expectations of PGE.

Stephanie Douglas

Stephanie Douglas