GRIDLIANCE

NOMAN WILLIAMS
Chief Operating Officer

PUBLIC VERSION

March 14, 2017

GridLiance Comments on the CAISO 2017-2018 Draft Transmission Plan

Need to Study Loss Contingencies for "Regional Hubs"

GridLiance West Transco LLC (GridLiance) provides these comments confidentially on an important reliability issue related to security of the Mead Regional hub. We respectfully recommend this issue be considered by the CAISO in the 2017-2018 Transmission Planning Process. The [redacted] sub-regional hubs of [redacted] are not only considered to be overly congested from a power flow perspective, but also highly physically constrained. Congestion in this area, which impacts the region economically and creates reliability issues, cannot be easily addressed given there is little or no room for expansion of these [redacted] existing substations beyond their currently installed, or recently-approved facilities.

The congestion and physical constraints, combined with a rapid expansion of utility-scale renewable [redacted] projects within this region, has resulted in a troubling concentration of critical power assets connected to the [redacted]. These assets depend on transmission that traverses a highly constrained physical path located in a narrow geographic and environmentally sensitive corridor to deliver power reliably. These critical power assets include thousands of megawatts of dispatchable (i.e., non-intermittent) generating stations such as [redacted] that are either located within, or connected to, [redacted]. Apart from the economic implications of the constrained path, there is a significant reliability issue that needs to be addressed. Namely, a natural disaster, a willful act of terrorism, or even an inadvertent action by a system operator could prove to be a catalyst for an extended blackout directly affecting [redacted], inclusive of [redacted]. Additionally, depending upon seasonal timing (and especially if the timing coincides with other emergent problematic issues with generation or system conditions), it is conceivable a super-regional cascading event could be initiated, with catastrophic results for the population, economic activity, and national security.

GridLiance is concerned that CAISO and others typically study the system under a single contingency scenario, and have only recently been required to study the loss of an entire facility. Despite these welcomed advances, no analysis has been completed that contemplates the loss of a regional hub such as [redacted]. Against the backdrop of the 2017-2018 TPP, we believe this is the perfect time to study the loss of all or part of [redacted]. The need to study the loss of "regional hubs" at [redacted] is rapidly gaining the attention of various local, state and federal agencies and legislators. These policymakers are focusing on the need to identify areas which are the most vulnerable to either natural events or the purposeful actions of bad actors. There is a growing concern that bad actors, including nation states, seek to disrupt our integrated power system – thereby creating national security crises, including the possible loss of life.

While it has been known for many years that systemic vulnerabilities exist within a vast high voltage network, especially one as compact and close in proximity as those related to [redacted], very little has been done to address this ever-growing danger beyond federal legislative action to mitigate this widely-documented weakness. This is despite innumerable articles, studies, reports, debates and findings

showing a significant risk to our national security and impact to our national economic viability, including the health and safety of the population. Such studies / reports include:

DATE	ARTICLE / URL
August 8, 2005	*Designation of National Interest Electric Transmission Corridors As Authorized by the Energy Policy Act of 2005,* National Interest Electric Transmission Corridor, *available at* https://energy.gov/sites/prod/files/edg/media/NIETC_Fact_Sheet.pdf
Nov 2012	*Terrorism and the Electric Power Delivery System*, The National Academy of Sciences, *available at* http://sites.nationalacademies.org/cs/groups/depssite/documents/webpage/deps_073368.pdf
April 2012	[redacted]
June 17, 2014	*Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations*, Congressional Research Service, *available at* https://fas.org/sgp/crs/homesec/R43604.pdf
July 2014	*Securing the U.S. Electrical Grid - Understanding the Threats to the Most Critical of Critical Infrastructure, While Securing a Changing Grid*, Center for the Study of the Presidency & Congress, *available at* https://thepresidency.org/sites/default/files/Grid%20Report%20July%2015%20First%20Edition.pdf
April 2016	[redacted]
April 11, 2016	*Memorandum, Testimony – Blackout! Are we Prepared to Manage the Aftermath of a Cyber-Attack or Other Failure of the Electrical Grid?*, Congressional Research Service, *available at* http://transportation.house.gov/uploadedfiles/2016-04-14-campbell.pdf
June 2016	J. Michael Barrett, *Challenges and Requirements for Tomorrow's Electrical Power Grid,* Lexington Institute – Future of the Power Grid Series, *available at* http://lexingtoninstitute.org/wp-content/uploads/2016/09/Tomorrows-Electrical-Power-Grid.pdf
Dec 2016	*Joint United States-Canada Electric Grid Security and Resilience Strategy*, Governments of the United States and Canada, *available at* https://www.whitehouse.gov/sites/whitehouse.gov/files/images/Joint_US_Canada_Grid_Strategy_06Dec2016.pdf
Dec 2016	*National Electric Grid Security and Resilience Action Plan,* Executive Office of the President, *available at* https://www.whitehouse.gov/sites/whitehouse.gov/files/images/National_Electric_Grid_Action_Plan_06Dec2016.pdf
Mar 2017	Presentation - ERCOT CIP WG – Security Trends Document Attached.

Regional Hub Considerations

[redacted] serves as a significant gateway for the delivery of vast amounts of power to [redacted]; therefore, its security is paramount. Yet [redacted] is at, or potentially, over capacity if the traditional bulk power delivery paths are relied upon. The concentration of these assets and transmission paths in existing

substations is economically beneficial to the rate payer, but GridLiance believes the time has come to consider the potential for catastrophic events should [redacted] be attacked or incapacitated.

GridLiance respectfully submits that it is in the interests of [redacted], as well as national security, to begin the process of further diversifying the physical path for import and export of generation between [redacted], rather than continuing reliance solely on [redacted].

[redacted]

[redacted] has well-documented opportunities[redacted] to deliver a wide range of abundant renewable power directly [redacted] and, at the same time, directly address grid security issues stemming from the possible incapacitation of [redacted]. [redacted]

Summary

To summarize, in addition to studying solutions for typical reliability, economic, and public policy needs, GridLiance believes the CAISO should include in future studies the possibility of an outage affecting [redacted] and mechanisms ensuring continued reliability [redacted] the event of the loss of that interface. [redacted] The key is to recognize and to develop a plan of action that reduces the reliance on [redacted]. By including scenarios such as the ones outlined above in its models and analyses, CAISO would be advancing an important policy objective that could positively impact[redacted] by avoiding a debilitating loss of power.

Respectfully Submitted by:

Noman L. Williams
Senior Vice President, Operations & Engineering and
Chief Operating Officer

GridLiance advisors who assisted in preparing these comments:

Terry Boston
Dave Hilt
Mike Stefanik

E-ISAC
ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

TLP: GREEN

ERCOT CIP WG – Mar. 2017

Current Security Trends

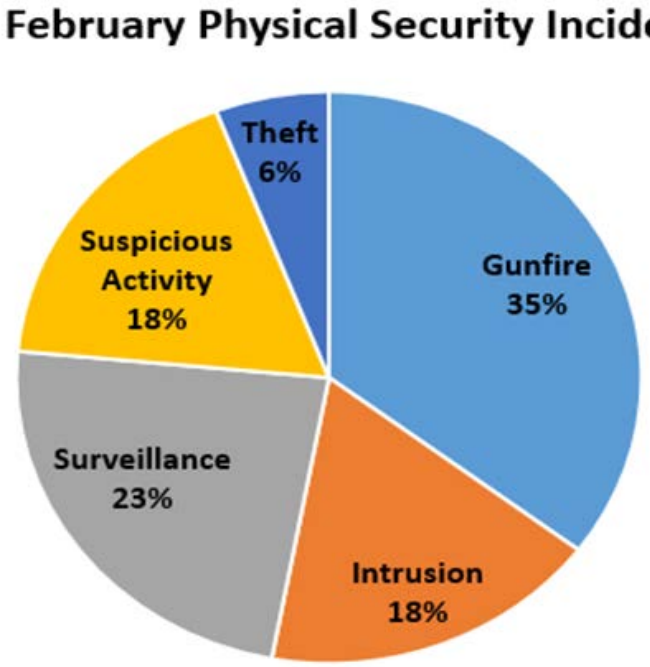
Joseph Januszewski, Senior Advisor
Charlotte de Sibert, Principal Physical Security Specialist
E-ISAC
March 3, 2017

RESILIENCY | RELIABILITY | SECURITY




- Current Trends
  - Cisco Industrial Routers and Security Appliance Failures
    - Cisco Industrial Security Appliances ISA-3000-2C2F-K9 and ISA-3000-4C-K9, and
    - Cisco IR809G-LTE and IR829GW-LTE Industrial Integrated Services Routers
    - *http://www.cisco.com/c/en/us/support/web/clock-signal.html*
  - Siemens RuggedCom NMS Vulnerabilities
    - CROSS-SITE REQUEST FORGERY (CSRF) and CROSS-SITE SCRIPTING (XSS)
  - Further Analysis of Shamoon2 Conducted
    - Symantec analysis (W23.Disttrack.B) indicates selected organizations in wider campaign
  - Phishing
    - Highlighting C-suite spear phishing

- Sector Trends
  - Phishing
    - Targeted Spear phishing
    - Embedded malware (PowerShell, etc.)
  - Credential harvesting
  - Password Cracking (Brute Force)
- New Threats
  - WordPress Vulnerabilities
- Physical
  - Gunfire
  - Surveillance
    - Photography, suspicious individuals, vehicle drive-bys etc.
    - UAS as surveillance method
  - Social engineering telephone calls



Analysis: Gunfire

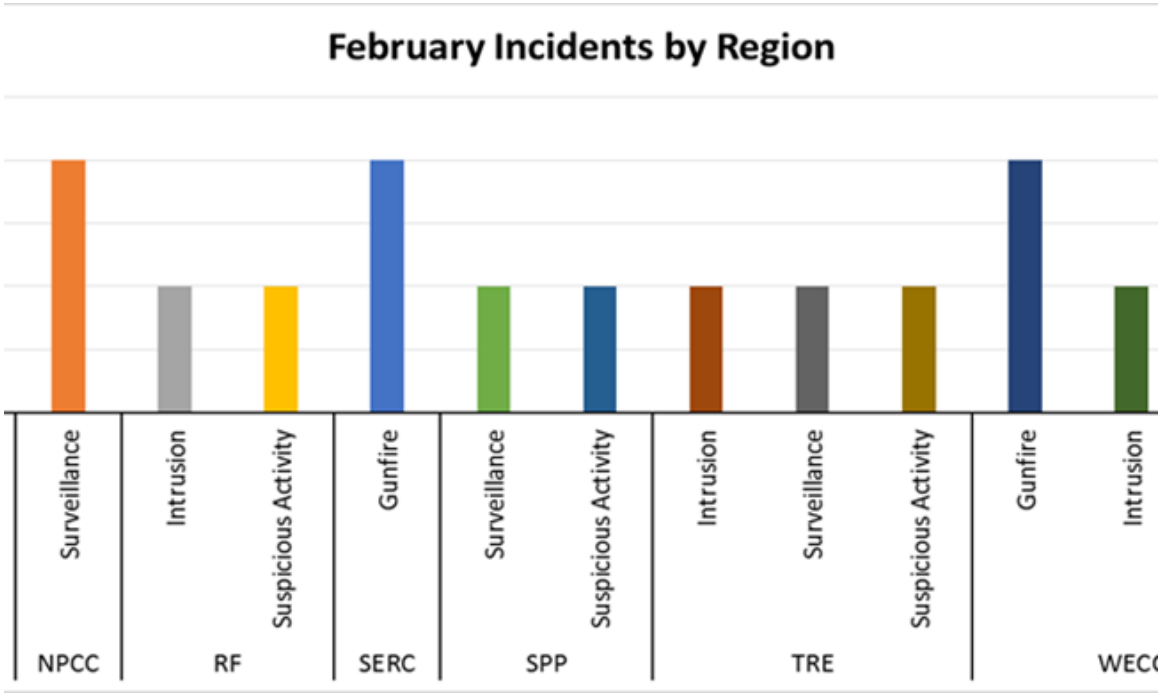
- Gunfire was the most reported event this month
- Incidents were unrelated
- Incidents predominantly occurred in remote areas
- Suspected that individuals are targeting facilities for target practice

Analysis: Surveillance

- 4 incidents occurred in the same week
  - Incidents were unrelated
- Report all events, details help ascertain threats and allow analysts to “connect the dots”

Regional Analysis

February physical security incidents, broken down by region, is displayed in the graph below.



Increase of reporting from ERCOT

- More data = a more accurate threat picture
- Does not impact E-ISAC view of grid security

For physical incidents or questions, please contact Charlotte de Sibert - Physicalsecurity@eisac.com

- Government Reports
  - DHS GrizzlySteppe Analytical Report
  - NIST Draft Special Pub 1800-7, Situational Awareness for Electric Utilities
  - GAO Report ELECTRICITY: Federal Efforts to Enhance Grid Resilience (GAO-17-153)

- E-ISAC Functions
  - E-ISAC Annual Report
  - Monthly Briefing (First Tuesday – March 7th)
  - Cyber Risk Preparedness Assessment & E2/C2M2 Workshop at SANS ICS (March 19th, Orlando, FL)

Questions and Answers