

Robert L. McGee, Jr.
Regulatory & Pricing Manager

One Energy Place
Pensacola, Florida 32520-0780

Tel 850.444.6530
Fax 850.444.6026
RLMCGEE@southernco.com



November 25, 2014

REDACTED

Ms. Carlotta Stauffer, Commission Clerk
Florida Public Service Commission
2540 Shumard Oak Boulevard
Tallahassee, FL 32399-0850

RECEIVED-FPSC
14 DEC - 1 AM 10:39
COMMISSION
CLERK

Dear Ms. Stauffer:

RE: Review of Physical Security Protection of Utility Substations and Control Centers

Enclosed is Gulf Power Company's Request for Confidential Classification regarding certain information submitted by Gulf Power in connection with Commission Staff's audit referenced above. Also enclosed is a CD containing Gulf's Request for Confidential Classification as well as Exhibit C in Microsoft Word as prepared on a Windows based computer.

Sincerely,

Robert L. McGee, Jr.
Regulatory and Pricing Manager

md

Enclosures

cc: Beggs & Lane
Jeffrey A. Stone, Esq.

COM _____
AFD _____
APA CD + Redacted
ECO _____
ENG _____
GCL _____
IDM _____
TEL _____
CLK _____

BEFORE THE FLORIDA PUBLIC SERVICE COMMISSION

IN RE: Review of Gulf Power Company's
Physical Security of Utility Substations and
Control Centers

Docket No.: Undocketed
Date: November 25th, 2014

REQUEST FOR CONFIDENTIAL CLASSIFICATION

GULF POWER COMPANY ["Gulf Power", "Gulf", or the "Company"], by and through its undersigned attorneys and pursuant to Rule 25-22.006, Florida Administrative Code, hereby files a request that the Florida Public Service Commission enter an order protecting from public disclosure certain information included in Gulf Power's responses to Commission Staff's data requests and in Commission Staff's workpapers concerning the Commission's Review of Gulf Power Company's Physical Security of Utility Substations and Control Centers (the "Review"). As grounds for this request, the Company states:

1. On May 8, 2014, Commission Staff initiated its Review. The Review addresses Gulf Power's plans and efforts toward preventing, detecting and recovering from deliberate physical attacks on the Company's substations and system control facilities. In connection with the Review Gulf Power produced detailed data concerning its transmission and distribution infrastructure and its plans and procedures for protecting the same against physical and cyber-attack. Securing and protecting its infrastructure is a top priority for Gulf Power and the Southern Company. The data produced by Gulf reveals a wealth of information regarding Gulf's security measures, systems and procedures. Moreover, portions of this information fit within the definition of confidential "critical energy infrastructure information" as defined by the Federal Energy Regulatory Commission ("FERC") regulation 338.113. The regulation defines critical energy infrastructure information as:

“[s]pecific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure that:

- (i) Relates details about the production, generation, transportation, transmission, or distribution of energy;
- (ii) Could be useful to a person in planning an attack on critical infrastructure;
- (iii) Is exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C. 552; and
- (iv) Does not simply give the general location of the critical infrastructure.”

18 C.F.R. 388.113(a)(1).

Critical infrastructure is, in turn, defined as “[e]xisting and proposed systems and assets, whether physical or virtual, the incapacity or destruction of which would negatively affect security, economic security, public health or safety, or any combination of those matters.” 18 C.F.R. 388.113(2).

Public disclosure of the subject information would enable potential wrongdoers to identify points of interest for their efforts and potentially undermine the integrity of Gulf Power’s transmission and distribution infrastructure. It is for this reason that information of this nature is entitled to confidential classification under section 366.093(3), Florida Statutes and is also recognized as exempt from public disclosure by the FERC.

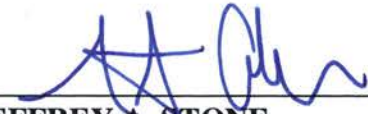
2. The information filed pursuant to this request is intended to be, and is treated as, confidential by Gulf Power and, to this attorney’s knowledge, has not been otherwise publicly disclosed.

3. Submitted as Exhibit "A" is one copy of Staff’s draft report. The information for which confidential classification is requested is highlighted in yellow. Exhibit "A" should be

treated as confidential pending a ruling on this request. Attached as Exhibit "B" are two (2) edited copies of the draft report, which may be made available for public review and inspection. Attached as Exhibit "C" to this request is a line-by-line/field-by-field justification for the request for confidential classification.

WHEREFORE, Gulf Power Company respectfully requests that the Commission enter an order protecting the information highlighted on Exhibit "A" from public disclosure as proprietary confidential business information.

Respectfully submitted this 24th day of November, 2014.



JEFFREY A. STONE
Florida Bar No. 325953
RUSSELL A. BADDERS
Florida Bar No. 007455
STEVEN R. GRIFFIN
Florida Bar No. 0627569
Beggs & Lane
P. O. Box 12950
Pensacola, FL 32591
(850) 432-2451
Attorneys for Gulf Power Company

BEFORE THE FLORIDA PUBLIC SERVICE COMMISSION

IN RE: Review of Gulf Power Company's
Physical Security of Utility Substations and
Control Centers

Docket No.: Undocketed
Date: November 25th, 2014

_____)


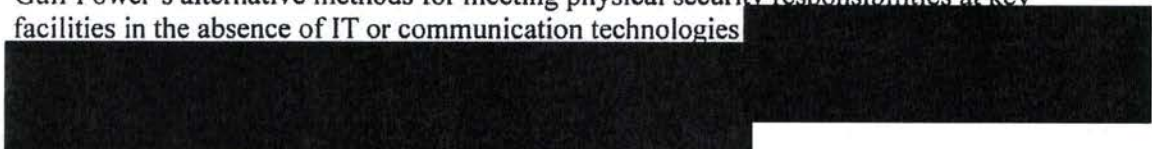
REQUEST FOR CONFIDENTIAL CLASSIFICATION

EXHIBIT "A"

Provided to the Commission Clerk under separate cover as confidential
information.

EXHIBIT "B"

RESPONSE:

- a. For those assets that have been identified as key to the bulk electric system (BES) reliability, the Company employs layered physical security measures commensurate with a “defense-in-depth” approach.

 - b. Gulf performs risk assessments as part of business assurance and disaster recovery planning processes where the use of service providers and their ready availability is included in the evaluation of response processes and plans, and in determining the Company’s ability to quickly avoid or mitigate any adverse or unforeseen events that could impact critical facilities. In addition to the emergency response plans and incident responses teams, Gulf’s business assurance program also includes business continuity plans which contain notification to stakeholders, identification of alternate work locations and needs, and employee and vendor contact lists to ensure provision of service (including by key interdependent service providers) with respect to business-critical functions.
 - c. Gulf Power’s alternative methods for meeting physical security responsibilities at key facilities in the absence of IT or communication technologies

- 7.
- a. Please describe your interactions with the Department of Homeland Security, FERC, Department of Energy, FBI or other federal agencies regarding assistance with or cooperation in physical security.
 - b. Has your company conducted a physical security evaluation of key assets in concert with the Department of Homeland Security or other federal agencies? Please describe.
 - c. Has your company conducted a physical or cybersecurity program maturity model assessment on its own or in cooperation with any federal agency? (For example, C2M2 FERC assessment) Please describe.

RESPONSE:

- a. Gulf Power interacts regularly with the Department of Homeland Security, the Federal Bureau of Investigation, the Florida Department of Law Enforcement (FDLE), and local law

CIP Standards, the physical security requirements mandate integration between physical security protections and the requirements for cyber security incident response.

12. What actions have been taken or planned by your company in response to the PG&E Metcalf substation attack?

RESPONSE:

Gulf, in coordination with the Southern Company Security Council and Southern Company Services Transmission, is participating in the CIP-014 physical security standards development process directed by NERC to identify and protect transmission substations and their associated primary control centers. In addition, the Southern Company Security Council, which is presently chaired by a Gulf employee,

[REDACTED] and, is engaged in an immediate review of appropriate physical security standards for all critical transmission substations across the Southern electric system.

13. a. Please describe your use of random security measures in your approach to physical security.
b. Please describe whether and how security measures are uniform versus tailored to each location.

RESPONSE:

- a. Random security measures are often deployed as a result of an upcoming event, a change in circumstances, a threat or past incident. In these instances, Gulf has initiated random security measures that [REDACTED] and the use of certain investigative techniques and other security measures to assist in security efforts.
- b. While there is a level of consistency of basic security measures across the system, overall security is tailored to each location based on the nature of the threat and the assessment of risk and vulnerability.

14. Please describe whether your company has identified how long it can operate without specific critical components and the likely timetables for replacement of them.

RESPONSE:

Gulf plans and operates its transmission system in accordance with NERC reliability standards. NERC Transmission Planning Standards, TPL 1 through 4, establishes planning criteria to assess bulk electric system performance to ensure that the BES can be operated to supply projected customer demands and projected firm transmission services for various contingencies identified in the standards. These contingencies include the loss of system components.

In addition, [REDACTED]

[REDACTED] Please refer to page 1, paragraph 4 of the attached introductory narrative for more information.

15. a. Please describe whether and how “denial of access” scenarios are built into the company’s response plans for key facilities.
b. Please describe whether and how plans have been made to deal with scenarios such as direct threats received, handling of heightened alerts from government agencies and immediate response to an attack on another utility (whether interconnected or not interconnected).

RESPONSE:

- a. At all key facilities, measures have been implemented to restrict physical access to authorized personnel. [REDACTED]

- b. Gulf has a Security Threat Level Change Procedure for dealing with direct threats to the Company’s physical assets and alerts from government agencies where a significant or credible threat may have an impact on the Company’s assets.

The threat levels used by the company internally are similar to those used by the National Terrorism Advisory System (NTAS). Per Gulf’s procedure, a Normal Threat Level is when no known threat to the Company’s physical assets exists or only a general concern exists about threats to physical or assets. An Elevated Threat Level is declared when a significant or credible threat may have an impact on the Company’s physical assets and an Imminent

Reliability Standards is defined by the Ethics and Compliance Corporate Framework Manual that presents a framework for establishing and maintaining sound compliance programs.

19. Please describe any other pro-active physical security initiatives by your company that go beyond regulatory or standard compliance activities.

RESPONSE:

Based on risk assessments, [REDACTED]
[REDACTED] And, as previously discussed, [REDACTED]
[REDACTED]

20. How do you determine which systems, components, and functions get priority in regard to implementation of new physical security measures?

RESPONSE:

Implementation of new physical security measures are based on both risk assessments and regulatory requirements (i.e. CIP standards).

21. a. Please describe any role the company is playing in the development of CIP-014 physical security standards.
b. What steps has your company taken in anticipation of the adoption of CIP-014?
c. Please describe the company's view on the extent of applicability of CIP-014 standards to the company's distribution substations and systems.



RESPONSE:

- a. Southern Company Services, as an agent of Gulf, actively participated in the standard development process by direct participation in the April 1, 2014 NERC technical conference in Atlanta, GA, direct participation in all standard drafting team meetings; engagement with the NERC Standards Committee (SC), NERC staff, and FERC staff; and formal comment development through engagement with the EEI industry trade organization.

24. a. Are there third-party providers of services whose physical security controls are beyond the control of your organization?
b. How has your organization explored potential physical security vulnerabilities caused by third-party vendors?
c. Are the activities of third-party vendor personnel monitored during their access to certain company facilities? Please explain.

RESPONSE:

- a. Third-party providers must abide by and comply with all the requirements, terms, and conditions of the contract set forth by Gulf Power.
- b. Physical security plans address measures implemented in accordance with multiple standards, which covers a range of potential threats and vulnerabilities, in order to afford Gulf Company certain physical protections.
- c. Yes, in certain locations, third-party vendors are not permitted to have unescorted access. In those instances, Company personnel are present at all times to observe their actions.

In addition, alternative measures may include, but are not limited to, 


25. Please describe how third-party contractors are used in any aspect of your physical security plan.

RESPONSE:

Gulf Power utilizes a security contractor who provides security guard services at certain locations on a regular basis, and other locations on an as needed basis.

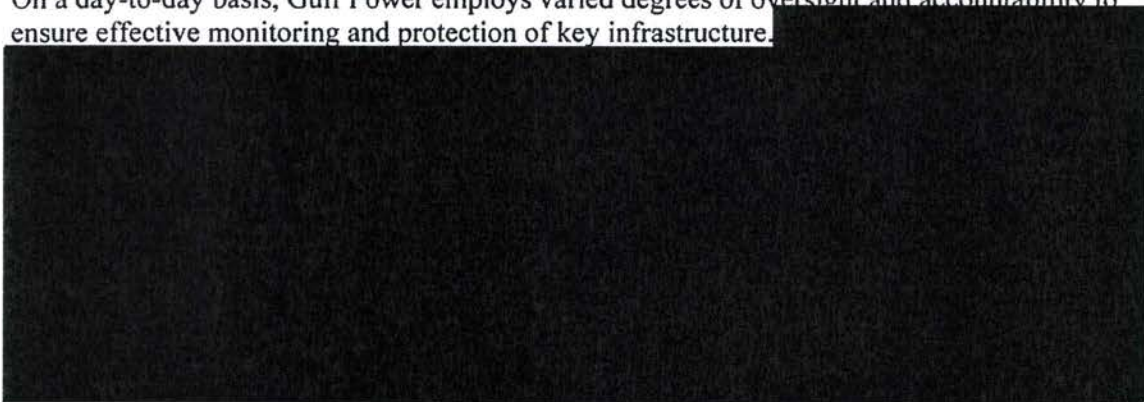
26. a. Please describe the distribution of responsibility for physical security among the company's operations and support work groups and corporate structure.
b. Please provide organizational charts.

RESPONSE:

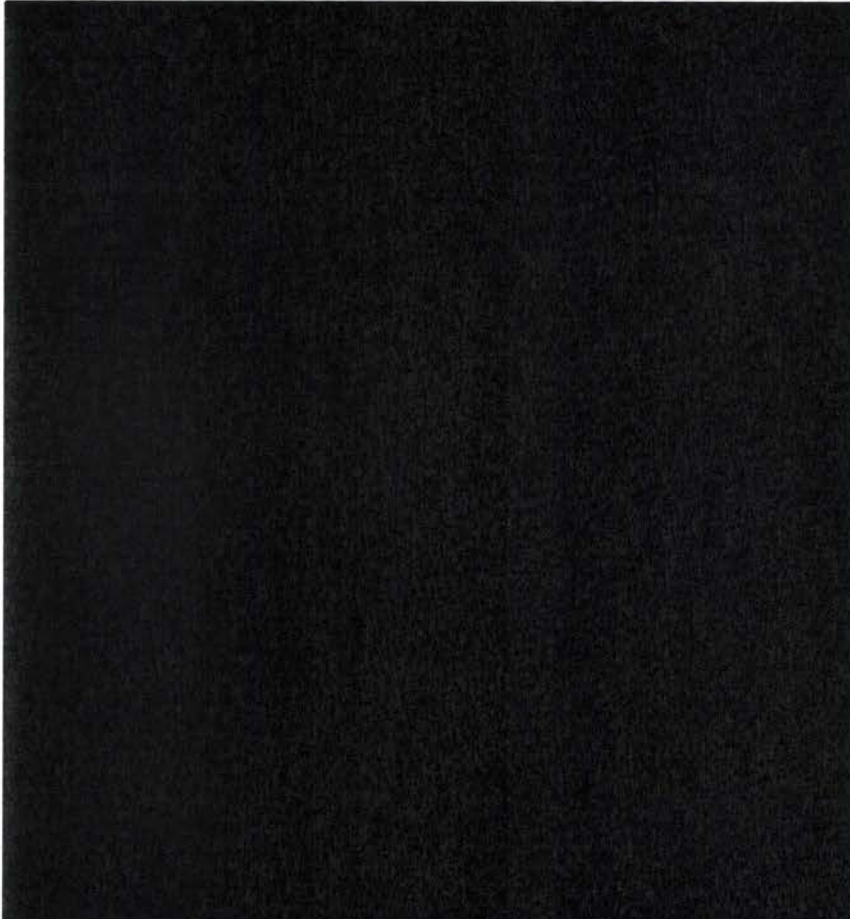
- a. The Corporate Security Department at Gulf Power has the responsibility of providing a secure environment and to protect the employees, processes and assets of the Company, but the message is clear that security is the responsibility of every employee. All employees are made aware of their responsibility with regards to situational awareness and their duty to act in reporting suspicious activity. Employees regularly receive training on incidents that might be anticipated, their inherent potential risks and the proper response in those situations. Periodic "There's No Security Without You" bulletins are also distributed to all employees to increase employee awareness and ownership of security in the workplace.

The Southern Company Security Council, comprised of all Southern Company Operating Companies and subsidiary Security Managers, meets regularly to discuss coordination, response, standardization, best practice, teamwork and being proactive in approach to security. At an executive level the Business Assurance Council, a management committee comprised of Operating Company and subsidiary Incident Response and Business Unit leaders and co-chaired by Southern Company's Chief Operating Officer and General Counsel, is charged with overseeing the Southern Companies' physical and cyber security policy activities in addition to recommending policies to help maintain business critical operations during unexpected disruptions.

On a day-to-day basis, Gulf Power employs varied degrees of oversight and accountability to ensure effective monitoring and protection of key infrastructure.



b.



27. a. Please describe the training provided to personnel who are involved with physical security.
- b. Please describe the physical security training provided to operations personnel of critical facilities.

RESPONSE:

a.



employees have received physical security related training from numerous sources including industry experts, security product vendors, law enforcement and peer training from other

employees with the same job responsibilities across the Southern Company. [REDACTED]

- b. Operations personnel receive training for substation and operating center access control. Annual NERC CIP training is required for all employees authorized to access CIP facilities.
- 28.
- a. Please describe any personnel surety/background checking performed for those with access to key physical components.
 - b. How are vendors and other third parties that have access to key physical assets screened?

RESPONSE:

Gulf requires several levels of personnel surety/background checks for those individuals with access to key physical components. During the pre-employment process, new employee screening may include, but is not limited to, verifying work and education history, a criminal background investigation and a drug screen. Company departments and organizations who utilize vendors are responsible for assigning the vendors into risk categories based on the services being performed. Certain risk categories require background investigations be performed on the vendors by Company approved providers before accessing company property or systems.

The Company utilizes a select group of personnel risk assessment providers that must comply with the strict background screening requirements that are established by the Company for both employees and vendors background investigations. These requirements include, but are not limited to, identity verification, criminal history checks and global watch lists.

Select areas of the Company must comply with the NERC CIP requirements in order to obtain access to these protected areas. All personnel (including employees, contractors, and/or vendors) that have a business justification for physical access to critical CIP sites or systems undergo a background investigation prior to being granted that access. In addition, those personnel must undergo a background investigation every seven years in order to retain that access as per the NERC CIP Standards.

- 29.
- a. For the most critical system components, are multiple operators required to implement changes that risk consequential events?
 - b. Describe what Change Management process is in place, especially in regard to systems which could present a risk to electrical reliability.

Corporation focused on testing the readiness and response of the industry to a major physical security attack. In 2012, Gulf conducted a terrorism tabletop drill involving armed invaders at one of our facilities in association with the FBI, DHS, FDLE and the RDSTF. In 2013, Gulf conducted a Hostile Intruder exercise with the FBI, DHS and the Pensacola Police Department (PD), utilizing a role player as an intruder and incorporating a response by the police SWAT team. Also in 2013, Gulf was a participant in GridEx II, an expanded national readiness exercise similar to GridEx I, incorporating both physical and cyber incidents in an effort to test worst-case response capabilities and readiness by the industry.

- b. In 2014, Gulf has planned another expanded Hostile Intruder drill in conjunction with the Pensacola PD, the Escambia County Sheriff's Office, the FBI and DHS.
31. Please describe provisions made to facilitate and maintain communication with federal, state, and local authorities following a physical attack.

RESPONSE:

Gulf employees have specific contact/liaison assignments with various Federal, state and local entities that have been incorporated into our Business Continuity/Storm plans. These relationships are cultivated and maintained throughout the year with personal visits, telephonic contacts and email exchanges to ensure appropriate communications capabilities during emergencies. In addition, [REDACTED] and the Security Manager at Gulf have specific liaison assignments with local, state and Federal law enforcement entities across the Gulf footprint with whom regular contact is made throughout the year.

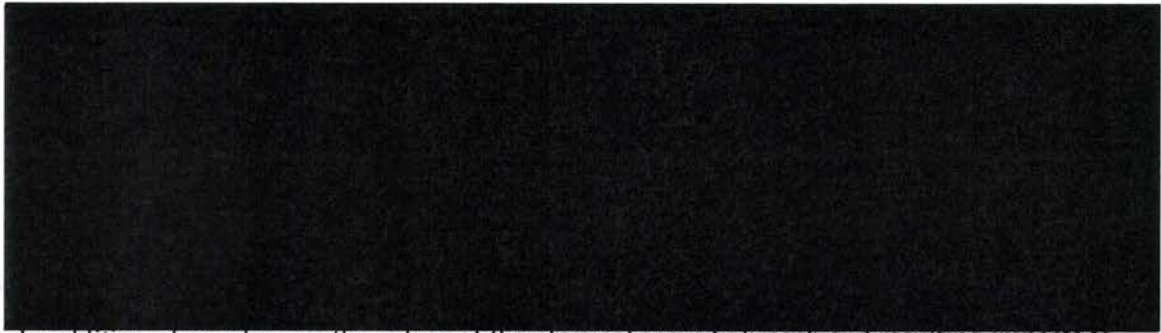


32. How are records kept of physical security access to key system components?

RESPONSE:

Records are kept electronically in the access control system database which retains information since the inception of the process for individuals with access to key system components. Manual logs are also maintained for escorted visitors to the Transmission Control Center.

33. a. What reporting occurs in the event of an attempted physical security breach, successful or not?
b. To whom is this report provided (internal and external)?
c. What reporting is required and what is courtesy reporting?

RESPONSE:

- 
- 
- 
- In addition, depending on the nature of the physical security breach and resulting impacts to the facility/system, the TCC and PCC may determine that the event requires the following:
 - Notification to the Department of Energy, using Form OE-417, for the “Physical attack that a) causes major interruptions or impacts to critical infrastructure or b) that could potentially impact electric system power adequacy or reliability; or vandalism which targets components of any security systems” event types.
 - Notification to NERC and SERC per Reliability Standard EOP-004-2 under the a) Damage or Destruction of a Facility, b) Physical Threat of a Facility, or c) Physical threat to a BES Control Center event types.
 - Notification to ES-ISAC per NERC CIP Standard CIP-008-3 for an actual physical security breach meeting certain conditions.
 - Notification to the internal Incident Response Team to determine if Security Threat Levels need to be changed which initiates activities on the system to enhance security and put the system in a safe and reliable posture.
 - Posting on the Reliability Coordinator Information System which shares the event with other Reliability Coordinators, NERC Situational Awareness, and SERC Situational Awareness.
 - The Southern Company Reliability Coordinator Operator may also provide a courtesy notification to the SERC Situational Awareness staff.

34. Please describe your established procedures for getting compromised structures back online.

RESPONSE:

Gulf Power Company is equipped and prepared to repair or replace damaged structures using normal operating and procurement practices. The Transmission Emergency Restoration Plan may be utilized to receive assistance from other Southern Company operating companies if needed for transmission emergency situations. In addition, procedures outlined in Gulf Power Company’s Storm Plan may be utilized if needed.

5. If not encompassed within question one, please provide the threat level guidelines referenced in Data Request 1.7.

RESPONSE:

See Gulf's response to question 1.

6. Please provide a listing of the 'points of contacts' noted in Data Request 1.10.

RESPONSE:

FERC

- Mike Bardee, Director of Reliability
- Gulf/Southern Company contacts are Noel Black and Wayne Moore

NERC

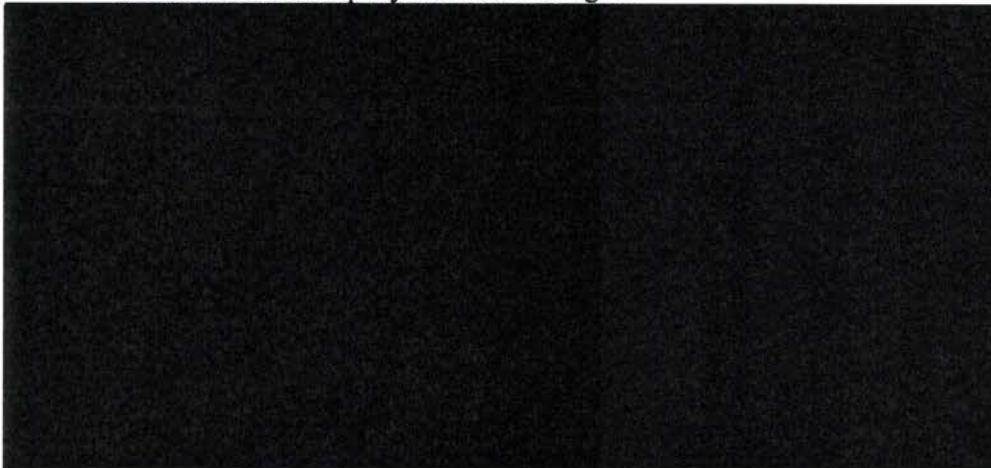
- Matt Blizard, Director of Critical Infrastructure Protection
- Gulf/Southern Company contact is Helen Nalley

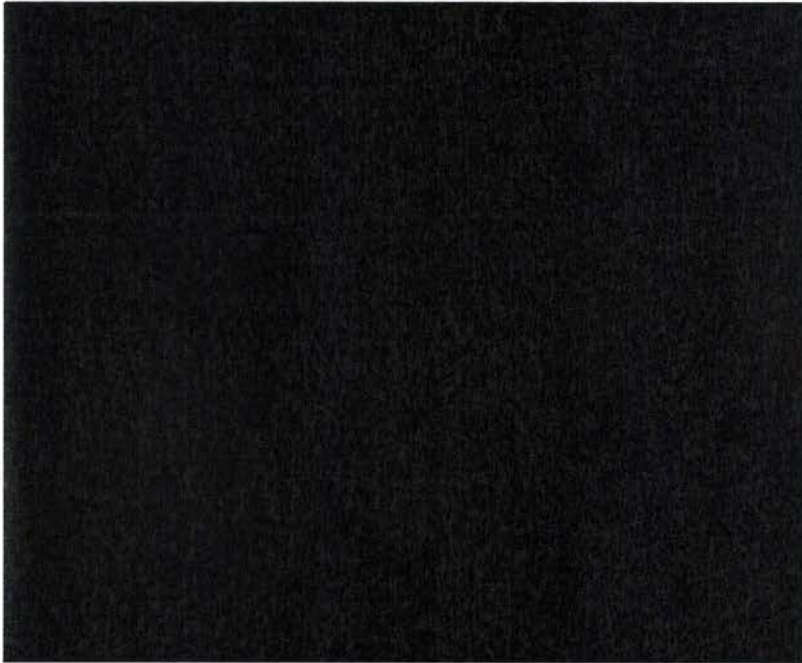
ES-ISAC

- Orlando Stevens, Desk Coordinator
- Gulf/Southern Company contact is Helen Nalley

ISC-CERT

- Lawrence K. Zelvin, National Cybersecurity and Communications Integration Center Director
- Gulf/Southern Company contact Joe Sagona





7. Please provide a member list for the *Southern Company Security Council* and each member's company title and affiliation.

RESPONSE:

Southern Company Security Council Core Members

George Schenck—Chairman—Security Manager, Gulf Power Company
David Guthrie—Vice Chairman—Security Manager, Southern Nuclear Company (SNC)
Randy Mayfield—Security Manager, Alabama Power Company (APC)
Steven Ford—Security Manager, Mississippi Power Company (MPC)
Philip Peacock—Security Manager, Georgia Power Company (GPC)

Southern Company Security Council Affiliate Members:

Jocelyn Stargel—Business Assurance Manager, Southern Company Services (SCS)
Bob Frisbee—Workplace Ethics and Compliance Director, SCS
Helen Nalley—Compliance Director, SCS
Luella Brown—Regional CIO, SCS
Kathy O'Shaughnessy—IT Security Manager, SCS
Kristie Barton—Transmission Maintenance General Manager, APC

Document #: 1-6
Date Requested: 5/8/14
Date Received: 6/9/14
Comments: (i.e., Confidential)

Document Title and Purpose of Review:

- a. How does your physical security plan include recognition of critical facilities and/or physical assets that are dependent upon IT or automated processing?
- b. How are interdependent service providers (for example, fuel suppliers, telecommunications providers, other outside vendors) included in risk assessments?
- c. How does your physical security plan include alternative methods for meeting critical functional responsibilities in the absence of IT or communication technology?

Summary of Contents:

a. For those assets that have been identified as key to the bulk electric system (BES) reliability, the Company employs layered physical security measures commensurate with a “defense in depth” approach



b. Gulf performs risk assessments as part of business assurance and disaster recovery planning processes where the use of service providers and their ready availability is included in the evaluation of response processes and plans, and in determining the Company’s ability to quickly avoid or mitigate any adverse or unforeseen events that could impact critical facilities. In addition to the emergency response plans and incident responses teams, Gulf’s business assurance program also includes business continuity plans which contain notification to stakeholders, identification of alternate work locations and needs, and employee and vendor contact lists to ensure provision of service (including by key interdependent service providers) with respect to business-critical functions.

c. Gulf Power’s alternative methods for meeting physical security responsibilities at key facilities in the absence of IT or communication technologies



Conclusions:

Data Request(s) Generated:

No. _____ Description:

No. _____ Description:

Follow-up Required:

Document #: 1-7

Document Title and Purpose of Review:

Division of Regulatory Compliance

Bureau of Performance Analysis

E:\Physical Security\Gulf\3.0 Work Papers\3.3 Document Summaries\Gulf DR1 Summary.doc

	<p>Conclusions:</p> <p>Data Request(s) Generated: No. _____ Description: No. _____ Description:</p> <p>Follow-up Required:</p>
<p>Document #: 1-12 Date Requested: 5/8/14 Date Received: 6/9/14 Comments: (i.e., Confidential)</p> <p>Confidential</p>	<p>Document Title and Purpose of Review: What actions have been taken or planned by your company in response to the PG&E Metcalf substation attack?</p> <p>Summary of Contents: Gulf, in coordination with the Southern Company Security Council and Southern Company Services Transmission, is participating in the CIP-014 physical security standards development process directed by NERC to identify and protect transmission substations and their associated primary control centers. In addition, the Southern Company Security Council, which is presently chaired by a Gulf employee, [REDACTED]</p> <p>[REDACTED]</p> <p>security standards for all critical transmission substations across the Southern electric system.</p> <p>Conclusions:</p> <p>Data Request(s) Generated: No. _____ Description: No. _____ Description:</p> <p>Follow-up Required:</p>
<p>Document #: 1-13 Date Requested: 5/8/14 Date Received: 6/9/14 Comments: (i.e., Confidential)</p> <p>Confidential</p>	<p>Document Title and Purpose of Review:</p> <p>a. Please describe your use of random security measures in your approach to physical security.</p> <p>b. Please describe whether and how security measures are uniform versus tailored to each location.</p> <p>Summary of Contents: a. Random security measures are often deployed as a result of an upcoming event, a change in circumstances, a threat or past incident. In these instances, [REDACTED]</p>

	<p>[REDACTED] the use of certain investigative techniques and other security measures to assist in security efforts.</p> <p>b. While there is a level of consistency of basic security measures across the system, overall security is tailored to each location based on the nature of the threat and the assessment of risk and vulnerability.</p> <p>Conclusions:</p> <p>Data Request(s) Generated: No. ____ Description: No. ____ Description:</p> <p>Follow-up Required:</p>
<p>Document #: 1-14 Date Requested: 5/8/14 Date Received: 6/9/14 Comments: (i.e., Confidential)</p>	<p>Document Title and Purpose of Review: Please describe whether your company has identified how long it can operate without specific critical components and the likely timetables for replacement of them.</p> <p>Summary of Contents: Gulf plans and operates its transmission system in accordance with NERC reliability standards. NERC Transmission Planning Standards, TPL 1 through 4, establishes planning criteria to assess bulk electric system performance to ensure that the BES can be operated to supply projected customer demands and projected firm transmission services for various contingencies identified in the standards. These contingencies include the loss of system components. In addition, Gulf has established processes and relationships to facilitate acquisition of spare equipment, including long lead time components such as transformers which are positioned strategically at select facilities and are available if needed. Please refer to page 1, paragraph 4 of the attached introductory narrative for more information.</p> <p>Conclusions:</p> <p>Data Request(s) Generated: No. ____ Description: No. ____ Description:</p> <p>Follow-up Required:</p>
<p>Document #: 1-15 Date Requested: 5/8/14 Date Received: 6/9/14 Comments: (i.e., Confidential)</p>	<p>Document Title and Purpose of Review:</p> <p>a. Please describe whether and how "denial of access" scenarios are built into the company's response plans for key facilities.</p> <p>b. Please describe whether and how plans have been made to deal with scenarios such as direct threats</p>

received, handling of heightened alerts from government agencies and immediate response to an attack on another utility (whether interconnected or not interconnected).

Summary of Contents:

a. At all key facilities, measures have been implemented to restrict physical access to authorized personnel. [REDACTED]


b. Gulf has a Security Threat Level Change Procedure for dealing with direct threats to the Company's physical assets and alerts from government agencies where a significant or credible threat may have an impact on the Company's assets.
The threat levels used by the company internally are similar to those used by the National Terrorism Advisory System (NTAS). Per Gulf's procedure, a Normal Threat Level is when no known threat to the Company's physical assets exists or only a general concern exists about threats to physical or assets. An Elevated Threat Level is declared when a significant or credible threat may have an impact on the Company's physical assets and an Imminent Threat Level is used when an attack against the Company's physical or assets has occurred or credible intelligence information indicates such an act is imminent.
Once made aware of an incident, an Incident Evaluation team is convened to assess the threat. If a decision is made to raise the Company's threat level, notification goes out to management and business units to activate the appropriate response and recovery plans. Gulf also has processes to respond to heightened alerts from government agencies that include threat evaluation, mitigation planning, and reporting.
Southern Company Services also has processes in place to communicate threats within the Southeastern Sub region of SERC to other utilities across NERC and to the Department of Homeland Security via the Reliability Coordinator Information System (RCIS) and to the Department of Energy through the Form OE-417 reporting. Southern also receives information relative to threats experienced by other utilities through the RCIS. In either case, whether experiencing a direct threat or being notified of another entity experiencing a threat, Southern notifies the Southern Company Services FBI contact for dissemination of information to the proper authorities and implements actions to put the system in a safe and reliable state.

Conclusions:


Data Request(s) Generated:

No. _____ Description:
No. _____ Description:

<p>Date Requested: 5/8/14 Date Received: 6/9/14 Comments: (i.e., Confidential)</p>	<p>Please describe any other pro-active physical security initiatives by your company that go beyond regulatory or standard compliance activities.</p> <p>Summary of Contents: Based on risk assessments, [REDACTED]</p> <p>Conclusions:</p> <p>Data Request(s) Generated: No. ____ Description: No. ____ Description:</p> <p>Follow-up Required:</p>
<p>Document #: 1-20 Date Requested: 5/8/14 Date Received: 6/9/14 Comments: (i.e., Confidential)</p> <p>Confidential</p>	<p>Document Title and Purpose of Review: How do you determine which systems, components, and functions get priority in regard to implementation of new physical security measures?</p> <p>Summary of Contents: Implementation of new physical security measures are based on both risk assessments and regulatory requirements (i.e. CIP standards).</p> <p>Conclusions:</p> <p>Data Request(s) Generated: No. ____ Description: No. ____ Description:</p> <p>Follow-up Required:</p>
<p>Document #: 1-21 Date Requested: 5/8/14 Date Received: 6/9/14 Comments: (i.e., Confidential)</p> <p>Confidential</p>	<p>Document Title and Purpose of Review:</p> <ol style="list-style-type: none"> Please describe any role the company is playing in the development of CIP-014 physical security standards. What steps has your company taken in anticipation of the adoption of CIP-014? Please describe the company's view on the extent of applicability of CIP-014 standards to the company's distribution substations and systems. <p>Summary of Contents:</p> <ol style="list-style-type: none"> Southern Company Services, as an agent of Gulf, actively participated in the standard development process by direct participation in the April 1, 2014 NERC technical conference in Atlanta, GA, direct participation in all standard drafting team meetings; engagement with

	<p>Summary of Contents: a. Vendors/Contractors are required to maintain complete documentation and records concerning compliance with all applicable legal requirements. Throughout the term of the contract, Vendors/Contractor shall maintain and permit Company representatives, during normal business hours, to examine, audit and make copies of all documentation and records of Vendor/Contractor, relating to compliance with applicable legal requirements. b. Project Managers or Contract Administrators serve as verifiers, and are required to attend Contract Manual training annually, or on an as needed basis.</p> <p>Conclusions:</p> <p>Data Request(s) Generated: No. _____ Description: No. _____ Description:</p> <p>Follow-up Required:</p>
<p>Document #: 1-24 Date Requested: 5/8/14 Date Received: 6/9/14 Comments: (i.e., Confidential)</p>	<p>Document Title and Purpose of Review:</p> <ol style="list-style-type: none"> Are there third-party providers of services whose physical security controls are beyond the control of your organization? How has your organization explored potential physical security vulnerabilities caused by third-party vendors? Are the activities of third-party vendor personnel monitored during their access to certain company facilities? Please explain. <p>Summary of Contents: Third-party providers must abide by and comply with all the requirements, terms, and conditions of the contract set forth by Gulf Power. b. Physical security plans address measures implemented in accordance with multiple standards, which covers a range of potential threats and vulnerabilities, in order to afford Gulf Company certain physical protections. c. Yes, in certain locations, third-party vendors are not permitted to have unescorted access. In those instances, Company personnel are present at all times to observe their actions.</p>  <p>Conclusions:</p> <p>Data Request(s) Generated:</p>

	<p>policy activities in addition to recommending policies to help maintain business critical operations during unexpected disruptions. On a day-to-day basis, Gulf Power employs varied degrees of oversight and accountability to ensure effective monitoring and protection of key infrastructure. [REDACTED]</p> <p>[REDACTED]</p> <p>Gulf provided a organizational chart.</p> <p>Conclusions:</p> <p>Data Request(s) Generated: No. _____ Description: No. _____ Description:</p> <p>Follow-up Required:</p>
<p>Document #: 1-27 Date Requested: 5/8/14 Date Received: 6/9/14 Comments: (i.e., Confidential)</p>	<p>Document Title and Purpose of Review:</p> <ol style="list-style-type: none"> a. Please describe the training provided to personnel who are involved with physical security. b. Please describe the physical security training provided to operations personnel of critical facilities. <p>Summary of Contents:</p> <p>a. Gulf Power Company has a Corporate Security Department which includes [REDACTED] Investigators and 1 Building and Asset Security Analyst [REDACTED]</p> <p>[REDACTED] These employees have received physical security related training from numerous sources including industry experts, security product vendors, law enforcement and peer training from other employees with the same job responsibilities across the Southern Company. In addition to this team, the Corporate Security Department manages a security control room which is staffed 24/7. These control room operators are trained to monitor and respond to physical security issues using multiple platforms and processes.</p>

	<p>relationships are cultivated and maintained throughout the year with personal visits, telephonic contacts and email exchanges to ensure appropriate communications capabilities during emergencies. In addition, each of the [REDACTED] Security Investigators and the Security Manager at Gulf have specific liaison assignments with local, state and Federal law enforcement entities across the Gulf footprint with whom regular contact is made throughout the year.</p>
	<p>Conclusions:</p>
	<p>Data Request(s) Generated: No. _____ Description: No. _____ Description:</p>
	<p>Follow-up Required:</p>
<p>Document #: 1-32 Date Requested: 5/8/14 Date Received: 6/9/14 Comments: (i.e., Confidential)</p>	<p>Document Title and Purpose of Review: How are records kept of physical security access to key system components?</p>
	<p>Summary of Contents: Records are kept electronically in the access control system database which retains information since the inception of the process for individuals with access to key system components. Manual logs are also maintained for escorted visitors to the Transmission Control Center.</p>
	<p>Conclusions:</p>
	<p>Data Request(s) Generated: No. _____ Description: No. _____ Description:</p>
	<p>Follow-up Required:</p>
<p>Document #: 1-33 Date Requested: 5/8/14 Date Received: 6/9/14 Comments: (i.e., Confidential)</p>	<p>Document Title and Purpose of Review:</p> <ol style="list-style-type: none"> What reporting occurs in the event of an attempted physical security breach, successful or not? To whom is this report provided (internal and external)? What reporting is required and what is courtesy reporting?
	<p>Summary of Contents: RESPONSE: </p>

- In addition, depending on the nature of the physical security breach and resulting impacts to the facility/system, the TCC and PCC may determine that the event requires the following:
- o Notification to the Department of Energy, using Form OE-417, for the “Physical attack that a) causes major interruptions or impacts to critical infrastructure or b) that could potentially impact electric system power adequacy or reliability; or vandalism which targets components of any security systems” event types.
 - o Notification to NERC and SERC per Reliability Standard EOP-004-2 under the a) Damage or Destruction of a Facility, b) Physical Threat of a Facility, or c) Physical threat to a BES Control Center event types.
 - o Notification to ES-ISAC per NERC CIP Standard CIP-008-3 for an actual physical security breach meeting certain conditions.
 - o Notification to the internal Incident Response Team to determine if Security Threat Levels need to be changed which initiates activities on the system to enhance security and put the system in a safe and reliable posture.
 - o Posting on the Reliability Coordinator Information System which shares the event with other Reliability Coordinators, NERC Situational Awareness, and SERC Situational Awareness.
 - o The Southern Company Reliability Coordinator Operator may also provide a courtesy notification to the SERC Situational Awareness staff.

Conclusions:

Data Request(s) Generated:

No. _____ Description:

No. _____ Description:

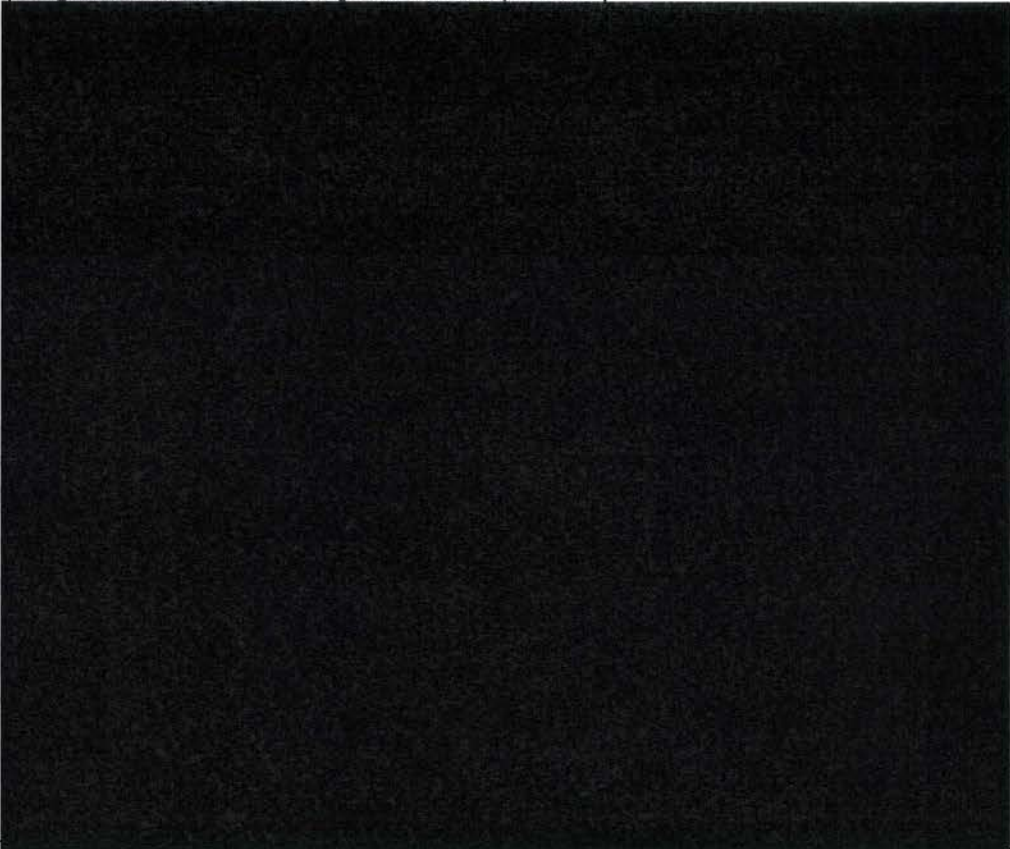
Follow-up Required:

Document #: 1-34
Date Requested: 5/8/14
Date Received: 6/9/14
Comments: (i.e., Confidential)

Document Title and Purpose of Review: Please describe your established procedures for getting compromised structures back online.

Summary of Contents:

Gulf Power Company is equipped and prepared to repair or replace damaged structures using

- Matt Blizard, Director of Critical Infrastructure Protection
 - Gulf/Southern Company contact is Helen Nalley
ES-ISAC
 - Orlando Stevens, Desk Coordinator
 - Gulf/Southern Company contact is Helen Nalley
ISC-CERT
 - Lawrence K. Zelvin, National Cybersecurity and Communications Integration Center
Director
 - Gulf/Southern Company contact Joe Sagona
Regional Domestic Security Task Force (RDSTF)
- 

Conclusions:		
Data Request(s) Generated:		
No. _____ Description:		
No. _____ Description:		
Follow-up Required:		
Document #: 2-7 Date Requested: Date Received: Comments: (i.e., Confidential)	Document Title and Purpose of Review: Please provide a member list for the <i>Southern Company Security Council</i> and each member's company title and affiliation.	
Summary of Contents: Southern Company Security Council Core Members George Schenck—Chairman—Security Manager, Gulf Power Company David Guthrie—Vice Chairman—Security Manager, Southern Nuclear Company (SNC) Randy Mayfield—Security Manager, Alabama Power Company (APC) Steven Ford—Security Manager, Mississippi Power Company (MPC) Philip Peacock—Security Manager, Georgia Power Company (GPC) Southern Company Security Council Affiliate Members: Jocelyn Stargel—Business Assurance Manager, Southern Company Services (SCS) Bob Frisbee—Workplace Ethics and Compliance Director, SCS Helen Nalley—Compliance Director, SCS Luella Brown—Regional CIO, SCS Kathy O'Shaughnessy—IT Security Manager, SCS Kristie Barton—Transmission Maintenance General Manager, APC		

**Bureau of Performance Analysis
Interview Summary**

Company: Area: Gulf Power Physical Security Auditor(s): Vinson, Coston, Delgado-Perusquia	Interview Number: 1 File Name: 3.5.1 INTERVIEWSUMMARY.DOC
Names: George Scherek-Security Manager Sharda Scott-System Operations Manager (23years) Rich Sanchez-Maintenance Manager-Transmission (25years) Steve Carter-Protections and Controls (22years) Steve Williams – Supply Chain Manager Lee Evens	Date of Interview: Location: Gulf Power Headquarters Telephone Number:

(1) Purpose of Interview: Discuss the company's approach to Physical Security of its substations and control centers.

(2) Interview Summary:

George Scherek is the Security Manager over the organization based in Pensacola. Has [redacted] investigators who work in the field monitoring all aspects of security (former FBI)

Sharda Scott is the system operations manager and transmission planning. Serves as the manager of the transmission control center and distribution control center.

Rich Sanchez is the transmission maintenance manager for the company and Steve Carter is the protection and controls group manager over CIP controls and protection of system.

Company presented a PowerPoint presentation on its overall physical security approach:
Prime areas of security—physical coverage/investigation/business assurance/training/law enforcement liaison/employee protection/uniform guards.

Changes since Metcalf: no changes to policy now...looking at risk evaluation and prioritization (risk-based site specific process. There were 11 briefings across country. No 'tags' of terrorist attack.

Lessons learned: Perimeter review in evaluation approach (Metcalf was outside attack)

Gulf looking at "new" technology—four companies on task force with ballistic fencing assessment

[redacted]
Southern Seven looking at issue

[redacted]
GridExII: Southern Co participated with around 1700 companies. Gulf was involved with Security Council in reviewing the scenario. GridExIII in 2015—will participate
In-house exercise in Oct 2013 for Gulf physical security of headquarters.
IRT exercise annually.

Risk assessment: can see live time/criminal activity/case management history
Total of 133 substations: 38 transmission/some have advanced security measures—Video IQ

Company made its own security assessments prior to CIP changes
Both Transmission and distribution has risk-based site specific threat assessment
Minimums security standards are the goal.

Communication with Federal include: Regional Domestic Security Task Force, FBI Joint terrorism Task Force, Fusion Center.

All SC companies have a Business Assurance Policy—includes all units with business critical functions. These units have to develop their own policy.

For power distribution, its mostly storm plan preparedness with physical security safeguards (10-11 departments have these plans)

EXHIBIT C

Line-by-Line/Field-by-Field Justification

Line(s)/Field(s)

Justification

Page 25, All highlighted data

Pages 28-29, All highlighted data

Page 32, All highlighted data

Page 34-37, All highlighted data

Pages 39-40, All highlighted data

Pages 44-45, All highlighted data

Page 57, All highlighted data

Pages 61-63, All highlighted data

Page 66, All highlighted data

Page 68, All highlighted data

Page 70, All highlighted data

Pages 74-75, All highlighted data

Pages 79-80, All highlighted data

Page 88, All highlighted data

This information is entitled to confidential classification pursuant to section 366.093(3)(c), Florida Statutes. The basis for this information being designated as confidential is more fully set forth in paragraph 1.