



Matthew R. Bernier  
Senior Counsel  
Duke Energy Florida, Inc.

December 1, 2014

**VIA HAND DELIVERY**

Mr. Jerry Hallenstein, Audit Manager  
Florida Public Service Commission  
2540 Shumard Oak Boulevard  
Tallahassee, Florida 32399-0850

**REDACTED**

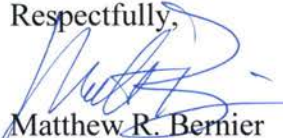
RECEIVED-FPSC  
14 DEC - 1 PM 4:48  
COMMISSION  
CLERK

Re: *Review of Physical Security Protection of Utility Substations and Control Centers;*  
*Undocketed*

Dear Mr. Hallenstein:

On December 1, 2014, Duke Energy Florida, Inc. ("DEF") filed an original and (7) copies of DEF's Request for Confidential Classification filed in connection with documents contained in Staff's Review of Physical Security Protection of Utility Substations and Control Centers Audit Control No. PA-14-5-003. Enclosed with this cover letter is DEF's confidential Exhibit A (in a separate sealed envelope) and two copies of redacted Exhibit B that accompany the above-referenced filing.

Thank you for your assistance in this matter. Please feel free to call me at (850) 521-1428 should you have any questions concerning this filing.

Respectfully,  
  
Matthew R. Bernier  
Senior Counsel

MRB/mw  
Enclosures

COM \_\_\_\_\_  
AFD \_\_\_\_\_  
APA 1 \_\_\_\_\_  
ECO \_\_\_\_\_  
ENG \_\_\_\_\_  
GCL \_\_\_\_\_  
IDM \_\_\_\_\_  
TEL \_\_\_\_\_  
CLK \_\_\_\_\_

# **Exhibit B**

**REDACTED**

Examples include [REDACTED]

### 3.2.1 RISK AND VULNERABILITY ASSESSMENTS

Critical cyber asset determination and assessments for DEF's transmission substations and system control center facilities are completed annually as part of the risk based assessment methodology required under NERC CIP-002. The latest assessment was completed in March 2014.

DEF currently uses Progress Energy's legacy risk analysis program to identify and prioritize the most serious potential vulnerabilities and security gaps in the Bulk Electric System. To do so, the following risk assessments are performed:

- ◆ Identify most critical Bulk Electric System facilities
- ◆ Estimate probability of threats occurring
- ◆ Estimate impact of a loss of a critical function or asset
- ◆ Document qualitative and quantitative measures used to determine impact levels
- ◆ Evaluate compliance with Physical Security Program procedures
- ◆ Identify controls to prevent or minimize the effects of potential loss.

After the assessments are completed, the risk analysis program tiers critical facilities in accordance to their importance to the reliability or operability of the electric grid. For example, tier 1 substations are those assessed to be the most critical to the company and if removed from the system or damaged would cause a serious or widespread outage.

For facilities designated as *critical* for CIP compliance purposes, both the Physical Security Perimeter and the Electronic Security Perimeter of the cyber asset are highly safeguarded. The Physical Security Perimeter is the six-wall "cube" (walls, ceiling, and floor) that houses the cyber asset. In most cases, the six-wall cube is either the control center or the control house building at a substation. These stations are required under CIP standards to employ security measures above DEF's baseline such as card readers, visitor logs, cameras, and video analytics. All critical and non-critical substations adhere to DEF's baseline security measures, which include a chain-linked fence, concrete block control house, lighting, and locks at station gate and control house."

Duke Energy's Enterprise Services Organization is currently in the process of integrating elements of Progress Energy's legacy risk analysis program into a new corporate *Work Place Security Policy*. The new Policy, to be published in November 2014, will standardize the risk assessment process for all of Duke Energy's service territory and will include procedures to comply with NERC's CIP-014 reliability standard regarding physical security.

To assess security protection, Duke Energy Corporation also monitors criminal activities that occur at its substations. **Exhibit 4** depicts 242 security incidents that occurred in DEF's transmission and distribution substations from 2011 through mid-July 2014. The vast majority of incidents (228) were burglary or theft related. Burglary incidents are those where substation perimeter intrusion was detected, whereas theft incidents are non-intrusive. The exhibit further shows the trend in the total number of incidents over time, from a high of 94 in 2011 to 62 in 2013. For 2014, only 11 incidents have been reported as of July 7.

DUKE ENERGY FLORIDA TRANSMISSION AND DISTRIBUTION SUBSTATION SECURITY INCIDENTS 2011-2014					
Types of Incidents	2011	2012	2013	2014*	Total
Burglary	51	53	27	3	134
Theft	41	22	24	7	94
Vandalism	2	0	11	1	14
<b>Total</b>	<b>94</b>	<b>75</b>	<b>62</b>	<b>11</b>	<b>242</b>

\*Through July 7, 2014.

**EXHIBIT 4**

Source: Document Request Response 3-1.

**3.2.2 PHYSICAL SECURITY INSPECTION PROCESS**

When warranted, corporate Enterprise Protective Services performs security inspections on its transmission substations. When determining which substations to inspect, corporate security considers factors such as new construction or the history of security incidents. The security inspections, also known as property security surveys, are thorough evaluations of existing security methods and systems based on minimum security standards as provided in the company's Physical Security Program procedures.

The inspection process includes, but is not limited to, an assessment of the perimeter fencing, substation structures, and electrical equipment. The final inspection reports include a description of the facility inspected, a brief history of security incidents, a security checklist to specify compliance by component (e.g., lighting and fencing), and recommended corrective action. A work order is to be generated for all deficiencies.

**3.3 DISTRIBUTION PHYSICAL SECURITY PROTECTION**

Distribution substations connect to the transmission system to reduce the transmission voltage, typically to about 30–60 kV, and terminate at a lower voltage below 1 kV at the customer's premise. DEF currently has 224 distribution substations that fall under the Commission's jurisdiction.

Like transmission substations, minimum physical security protection measures at distribution substations include [REDACTED]. If needed, security may be enhanced with features such as [REDACTED]. A disabled distribution substation can be rerouted in a fairly quick order with customer impacts avoided or limited. Therefore, distribution substations are not likely targets of attacks for the purpose of system disruption.

**3.3.1 RISK AND VULNERABILITY ASSESSMENTS**

Security protections in place at distribution substations are primarily deployed to mitigate against burglary/theft (often copper ground wire) and vandalism. Distribution substations are typically unmanned and thus somewhat more susceptible to unauthorized access. Risk and vulnerability assessments performed on DEF's distribution substations are primarily done in response to perceived potential weaknesses.

While physical security of all DEF's substations is on the company's radar, the company must answer the fundamental question of what are the most important assets to the organization. The primary driver, at this moment, for substation security is the regulatory push for implementation of CIP-014, requiring physical security protection of the most critical substations and control centers.

### 3.3.2 PHYSICAL SECURITY INSPECTION PROCESS

[REDACTED]

Distribution substation inspections are performed when requested by facilities management or if the need arises resulting from a security incident at the substation. During inspections, substation personnel are required to record any deficiencies for generation of work orders. Duke Energy senior management notes that the company's maintenance department inspects substation perimeter fencing as part of routine substation maintenance.

## 3.4 RECOVERY AND RESPONSE

DEF's operations are designed for redundancy and resiliency. DEF's transmission and distribution organizations both have documented recovery plans in place for emergencies whether caused by natural phenomena or other causes. Both transmission and distribution plans establish command and control structures to aid in communications and repair efforts. Both transmission and distribution control centers have backup capabilities and procedures in place. Per NERC Standard EOP-008, Duke must also maintain a fully redundant backup control center certified by both NERC and the FRCC.

Transmission and distribution recovery plans were developed for use when either catastrophic damage to facilities has occurred, or when a wide area severe weather warning, such as a hurricane, is issued. Both plans establish a consistent approach and level of responsibility for response by providing the authority and coordination needed to restore electric service and maintain business continuity. The plans are organized to consolidate authority to system level top down organizational structure for major storm responses and are appropriate for use in recovery from non-storm outages.

Duke Energy Corporation also has business continuity plans that describe response actions for loss of access to a critical facility. The plans are currently being updated to include elements provided in NERC's *Security Guideline for the Electricity Sub-Sector: Physical Security Response* (see Appendix 2). The *Security Guideline* provides utilities with actions they should consider when responding to threat alerts issued by the U.S. Department of Homeland Security and when operating during normal conditions. The updated business continuity plans will be included in new corporate *Work Place Security Policy* to be completed in November 2014.

Following the September 11, 2001 terrorist attacks, Duke Energy Corporation began participating in Edison Electric Institute's (EEI) Spare Transformer Equipment Program (STEP). The Program creates a sharing arrangement among electric utilities to make efficient use of existing transmission spare transformers. The lead time for the manufacture of large substation transformers is typically two years and most are manufactured overseas. The Program carries with it a binding obligation to provide transformers if called upon by another STEP participant.

**AUDIT WORKPLAN**  
**PHYSICAL SECURITY OF SUBSTATIONS AND CONTROL FACILITIES**  
**Duke Energy Florida WLCF 14-005-003**

No.	Task	Standard	Audit Notes
		lines should exist.	the Vice President of Administrative Services for Duke Energy Corporation. The Managing director is responsible for oversight of the following four business units, each headed by a director: Operational Security Investigations, Security Risk and Compliance, Infrastructure Protection, and Preparedness Services and Business Continuity.
6	Review internal facility risk assessments of transmission substations, distribution substations and control centers.	NERC CIPs 002 and 014 require identification of critical assets. Should be updated periodically. Should reflect revisions and additions to CIPs.	See DR1-2, 2-4, 3-4 and Interview Summ. For transmission substations: Property security surveys are thorough evaluations of existing security methods and systems based on minimum security standards as provided in the company's Physical Security Program procedures. For Distribution substations: distribution substation inspections are performed [REDACTED]
7	Review and assess efforts to respond to 2013 PG&E substation attack and lessons learned	Specific actions have been identified by PG&E than can be considered. Vendors are offering enhanced camera, lighting and intruder detection systems. Vegetation control and site visibility are viable considerations.	See DR1-12 and Interview Summ. Enterprise Protective Services personnel visited the Metcalf site to discuss lessons learned and best practices with Pacific Gas and Electric Company.
8	Determine what actions are planned as a result of 2013 PG&E substation attack	PG&E plans \$100 million physical security enhancements for substations over next 3 years for needs identified as result of the attack. Florida utilities should consider applicability. Virginia Dominion plans \$500 million in similar enhancements over 10 years.	See DR1-12 and Interview Summ. Duke Energy senior management determined that resources should be specifically dedicated to physical security protection. In 2014, a new business unit, Physical Security Projects, was created within the Enterprise Protective Services organization to oversee transmission physical security protection and the development and implementation of NERC's CIP-014 reliability standard.
8	Determine degree of effort given to consider long term implications of CIP-014 in distribution operations.	CIP-014 only applies to large transmission substations. However many of the activities and protections may have applicability to distribution operations, depending on risk and cost analyses.	SEE DR 1-21 and Interview Summ. Duke Energy has been an active participant in the development of the NERC CIP-014.. The company is currently evaluating different security technologies to be implemented to mitigate risk once the CIP-014 standard is finalized. The company is approaching CIP-014 in

	<p><b>Conclusions:</b></p> <p><b>Data Request(s) Generated:</b>  No. _____ Description: Obtain most recent FRCC audit  No. _____ Description:</p> <p><b>Follow-up Required:</b>  *See interview questions pertaining to the Physical Security Program Procedure  *Explain the review process of Enterprise Document Control Program. (see response to b)</p>
<p><b>Document #: 1-2</b>  <b>Date Requested: 5/8/14</b>  <b>Date Received: 6/9/14</b>  <b>Comments: (i.e., Confidential)</b></p>	<p><b>Document Title and Purpose of Review:</b></p> <ol style="list-style-type: none"> <li>a. Has your organization conducted a physical risk or vulnerability assessment of its transmission substations, distribution substations, and system control room facilities?</li> <li>b. How were these assessments conducted?</li> <li>c. Who conducted these assessments?</li> <li>d. How often are these assessments revisited or redone?</li> </ol> <p><b>Summary of Contents:</b></p> <ol style="list-style-type: none"> <li>a. Critical asset determination assessments of transmission substations and system control room facilities are completed annually as part of the Risk Based Assessment Methodology required under NERC CIP-002. The latest assessment was completed in March 2014. Vulnerability and consequence assessments were also completed as part of the Enterprise Business Critical Infrastructure ("BCI") Policy and Program (documentEMG-SUBS-00104) that required on-site assessments of Tier 1 (i.e. critical) facilities every 3 years per Section 6.6. This program is in transition since 2013 following the merger of Progress Energy with Duke Energy. The last assessments of Tier 1 sites [REDACTED] were conducted in 2011. Physical risk assessments of transmission substations not tiered under the BCI program have also been performed. Duke Energy is currently developing the methodology for conducting assessments as part of NERC CIP-014 proposed standards.</li> <li>b. The critical asset determination assessments were completed using the criteria established under NERC CIP-002. Physical risk assessments were completed per the Physical Security Program procedure (SEC-SUBS-00079).</li> <li>c. The critical asset determination assessments using CIP-002 criteria were completed annually by Duke Energy business units including Transmission and Information Technology. Physical security risk assessments were completed by Duke Energy Enterprise Protective Services.</li> </ol>

	<p>d. The critical asset determination assessments using the criteria established under NERC CIP-002 are performed annually. Regular assessments have not been completed on physical security risk assessments. Duke Energy's Enterprise Protective Services is working toward standardizing the physical security risk assessments process enterprise wide. The proposed NERC CIP-014 will drive reoccurring assessments every 30 months, 60 months, and 120 calendar days as outlined in proposed R1.1 and R5.</p> <p><b>Conclusions:</b></p> <p><b>Data Request(s) Generated:</b>  No. ____ Description: Obtain the last assessments of Tier 1 sites [REDACTED] were conducted in 2011  No. ____ Description:</p> <p><b>Follow-up Required:</b>  *Explain the vulnerability and consequence assessments completed as part of the Enterprise Business Critical Infrastructure ("BCI") Policy and Program (documentEMG-SUBS-00104) that required on-site assessments of Tier 1 (i.e. critical) facilities every 3 years per Section 6.6. (see response to a)  *Need to discuss the standardization of the physical security risk assessments process enterprise wide. (see response to d)</p>
<p><b>Document #: 1-3</b>  <b>Date Requested: 5/8/14</b>  <b>Date Received: 6/9/14</b>  <b>Comments: (i.e., Confidential)</b></p>	<p><b>Document Title and Purpose of Review:</b></p> <p>a. Has your physical security plan been reviewed in the last year and updated as needed?</p> <p>b. How often is it reviewed and updated?</p> <p><b>Summary of Contents:</b></p> <p>a. Those sites identified as critical under NERC CIP-002 have site specific physical security plans. These plans have been reviewed in the past year and updated as necessary.</p> <p>b. For the site specific security plans under NERC CIP-006-3c, they are reviewed and updated annually.</p> <p><b>Conclusions:</b></p> <p><b>Data Request(s) Generated:</b>  No. ____ Description:  No. ____ Description:</p> <p><b>Follow-up Required:</b>  *Identify the sites that are critical under NERC CIP-002</p>
<p><b>Document #: 1-4</b>  <b>Date Requested: 5/8/14</b></p>	<p><b>Document Title and Purpose of Review:</b></p>



	<p>communication with other agencies under NERC EOP-004-2</p> <p>b. Duke Energy Florida completed assessments of specific key assets with Department of Energy and US Secret Service supporting the Republican National Convention in 2012. [REDACTED]</p> <p>c. In preparation for the 2012 Democratic and Republican National Conventions being held in Charlotte, NC and Tampa, FL respectively. Duke Energy participated in a Department of Homeland Security led Cyber Resilience Review. Following that review, Duke Energy adopted the Electricity Subsector Cybersecurity Capability Maturity Mode! (ES-C2M2). In 2013, the Department of Energy and individuals from Carnegie Mellon met with Duke Energy to conduct the C2M2 assessment.</p>
	<p><b>Conclusions:</b></p>
	<p><b>Data Request(s) Generated:</b></p> <p>No. _____ Description: Obtain C2M2 Assessment that came out of Carnegie Mellon</p> <p>No. _____ Description:</p>
	<p><b>Follow-up Required:</b></p> <p>*Need explanation of communication protocols with FERC, DOE, FBI and local agencies. How is this documented? See answer to a</p> <p>*What key assets were assessed in support of the Republican National Convention? See answer to b</p> <p>*Need explanation of the Cyber Resilience Review. Was this documented? See answer to c</p> <p>*Need explanation of the ES-C2M2 . Is this documented?</p>
<p><b>Document #: 1-8</b>  <b>Date Requested: 5/8/14</b>  <b>Date Received: 6/9/14</b>  <b>Comments: (i.e., Confidential)</b></p>	<p><b>Document Title and Purpose of Review:</b> What is your company's process/plan for managing physical security-related risk? (Example: DOE/NIST/NERC Risk RMP)</p> <p><b>Summary of Contents:</b>  Duke Energy has an enterprise level physical security policy that outlines the Company's expectations and general responsibilities. The policy is supported by program procedures and guidance. The Physical Security Program Procedure (document SEC-SUBS-00079) describes physical security recommendations for all Company facilities and methods for conducting physical security evaluations of facilities. There are additional procedures that cover physical security controls for assets regulated under NERC CIP.</p> <p><b>Conclusions:</b></p> <p><b>Data Request(s) Generated:</b></p> <p>No. _____ Description:</p> <p>No. _____ Description:</p> <p><b>Follow-up Required:</b> See interview questions pertaining to the Physical Security Program Procedure</p>

## Bureau of Performance Analysis Interview Summary

Company: Duke Energy  
Area: Physical Security  
Auditor(s): Fisher/Hallenstein

Interview Number:  
File Name: 7/7/14-7/8/14

Name:  
Matt Bernier  
Tom Bowman  
Paula Gugino (Charlotte) C2M2 (Sarbanes)  
Nelson Peeler (V.P. system Operations—control center, training/engineering)  
Darren Meyers- (Charlotte) Reg. Security/Business Security  
Danielle Bennett –Legal State/Fed, NERC Corp. Compliance  
Glenn Dooley-(St. Pete) Director of Systems Control

Date of Interview: 7/10/14  
Location: St. Pete  
Telephone Number:

(1) Purpose of Interview: To develop an understanding of Duke's Physical Security Program and CIP standards.

(2) Interview Summary:

### CIP 2-11 Version 3

- Risk Based—Define on your own which assets are critical (version 3)
- cyber assets "essential" to operation of critical asset
- Used routable protocols or dial-up. If internal, not in scope

### CIP 2-11 Version 5

- Specifically defines list of areas to look at using a bright line criteria
- Three levels (high, medium, low)
- cyber assets/systems that if unavailable, within 15 minutes, could adversely impact the reliable operation of the BES
- Connectivity determines level of protection not applicability. All routable protocols (internal or external) are in scope

### Implementation of CIP Version 5

- April 1, 2016 (High and Medium Impact BES Cyber Systems)
- April 1, 2017 (Low impact BES Cyber Systems)
- \*\*\*Distribution Protection Systems can have low impact BES Cyber Systems---In other words, possible for distribution to come in under version 5 if distribution protects bulk grid\*\*\*

- Year and a half ---started a transformation program for merger across companies
- Duke used Ernest & Young as project manger for interpretations and transition of version 3 to version 5. Ernest & Young provided tech and audit support.
- pulled together cross-functional business unit (completed as of 6/1/14)

### CIP Audit

Basic CIP audit is:

- Critical cyber, electronic security protection (ESP), physical security, physical access, electronic monitoring across personnel, training, evidence sampling, RSOGS reliability standards, procedures etc, on-site walk downs,
- FRCC looks at NERC standards. Wants list of every person who has access to physical asset.
- Wants list of critical assets.
- Duke gives FRCC reliability worksheet and explains how duke is compliant.
- FRCC audit is both offsite and onsite.
- report consists of audit findings, concerns and recommendations.
- must provide mitigation report to FRCC, NERC, and FERC if violation. (FRCC files with NERC and NERC files then with FERC)

### CIP 14

- Start with bright line test (black start)
- substations greater than 500 KV (example)



- Information sharing and communications
- Event and incident response, continuity of operations
- supply chain and external dependencies management
- workforce management
- cybersecurity program management
- slide 16 of PowerPoint:
  - Duke Energy adopted ES-C2M2 model baseline current practices and to establish desired maturity levels across the ten domains.
  - Implementation involved legacy NERC CIP teams from Transmission, Generation, NERC Corporate Compliance, Information Technology, and Enterprise Protection Services and included the following activities.
    - Mapped NERC CIP Reliability Standards and Requirements to the domains in the model
    - Develop action items, prioritization and implementation plans
- Resiliency review was similar to C2M2 but was more about response
- Mapped to CIP standards where applicable
- Mapped C2M2 to physical security and started looking at what Duke needed to do in action plans and settlement to prior violations w/FRCC

DR1-7

- Worked Republican National Convention
  - both key transmission and distribution asset protection
  - At Tropicana Field
  - Tampa Fairgrounds
  - Assessed key infrastructure and reviewed security

CIP-08 covers cyber incident reporting

- EOP 4 Reported to DOE and NERC
  - reported if affects greater than 50,000 customers per hour
  - FPSC staff gets copies
- Incidents captured in case management system
  - Examples of incidents include security: theft, sabotage, arson, burglary
  - prior to merger, report sent to upper management. Now a monthly report to V.P. ?
- Tom Bowman will lead efforts for physical security under transmission (CIP 14)

Florida Assessments done in 2012 (approximately)

- Minimum standards are reviewed, performed by Corporate Security
  - BCI Oversight Committee-identifies resources, financial, and completing priorities
  - With CIP 14 there will be another level above current level.
- Tier 1 assessed on physical security and business continuity report

Organization (see org chart provided in DR and slide 6 of PowerPoint presentation)

- Enterprise Protective Services is a subset of Administration
- Tom Bowman will lead security assignment—physical security priorities (CIP 14)
  - “Thought it would be good to have dedicated resources after Metcalf incident”
- four units:
  - Business Continuity
  - Security Risk and Compliance
  - Investigations and Security
  - Infrastructure Protection Services
- Duke Protective Integrated Transmission Operations-Conducted Value Stream Analysis (VSA)
  - Responsibilities include:
    - CIP 14
    - Security work
    - Resiliency
    - Developing standard
    - Industry and research activities
    - Each stream will develop recommendations
- Functions:
  - Physical and technical security

- Corporate investigations
  - criminal, code of ethics
- Pre-employment screening
- Enterprise continuity
- Enterprise crisis management
- non-regulated drug and alcohol testing
- security regulatory compliance
- executive protection
- local, state, and federal law enforcement liaison

-2014 Major Focus Areas

- Cost control
- Implementation of CBE initiatives
- Regulatory compliance
  - Maritime Transportation Security Act (MTSA)
  - NERC Cyber Security Standards
- Contractor surety
- Perspective implementation
- Substation security
  - risk and vulnerability assessments
  - customer consultation

-2014 Major Focus for Enterprise Protective Services Florida Region

- Cost Control
- NERC implementation
  - NERC rules June 2013 required fully redundant "hot back-up" See EOP -008.
  - CIP 9- Requires that you have to have a detailed backup plan
- TSA pipeline security implementation
- Guard force reduction strategy
- FL crisis management team implementation
- Storm preparation
- Levy county support
- Threat management
- Guard force performance

-Fusion Center-Each jurisdiction has a fusion center (law enforcement is the driver)

- Enterprise Command Center -Monitors physical assets
  - Action item: put pisim monitors in control centers

Metcalf

- An event that FERC responded to by creating CIP 14
- Metcalf was able to maintain service even with damage
- Event occurred day after Boston Marathon bombing
- In October 2013 did review of substation security. Tome met with PG&E after Metcalf. Duke determined that it would be good to have dedicated resources to physical security after Metcalf incident.
- Lessons learned:

[REDACTED]

-Post Metcalf Incident Activities at Duke: (see PowerPoint Presentation page 9)

[REDACTED]

[REDACTED]

Incidents

[REDACTED]

STEP program

- Implemented about 5 years ago
- EEI member companies
- works in the form of a contractual agreement
- must keep a certain number and certain type of spares on hand (numbers are confidential)
- Question arises as to whether program should be expanded

Drills and Exercises

- GridEx – Is a primarily a government led cyber test communications exercise at the national level
  - Scenario exercise that last 2 or 3 days.
  - In 2013 went through what GridEx nationally done and is a test to check readiness
  - Next GridEx III to be conducted in the fall of 2015. (conducted every other year)
  - Reports available on website
- System Operation Training on sabotage awareness 2012-2014
  - Review of Metcalf event
  - Recognition (recognize that something odd is going on)
  - Reaction
  - Safety
  - CIP 8 and 9 require specific tests of incident reporting and recovery for cyber systems

7/8/14

-Sub 79-Physical Security Program (Darren)

- Security Coordinator performs risk/vulnerability.
  - looks for gaps and exposures against minimum standards. Recommends changes.
  - Report goes back to asset owner to make changes if necessary.
  - BCI was retired after merger but Duke is bringing it back. Important to bring back. [REDACTED]
  - BCI Oversight Committee-Determines appropriate dollars in right place.
    - As it relates to CIP 14, a budget for 2014 has been done for level 3 (high level). BCI is legacy Progress
  - Under BCI: [REDACTED]

- Darren: Would like to roll Workforce Security Policy and Physical Security Program into one policy
- Danielle: Today each facility in CIP version 3 in Florida has its own security plan (shown template for version 5)

Vendors

- Third party vendor source agreement Duke Florida uses standard design guide.
- Pre-employment investigation finds issues with vendor employees (7 year criminal, local, county, state)
  - If Vendor gets a badge, a background check is done on contracting company
  - Procedure went into affect August 1, 2013
- Very little turnover of security vendors
- When new equipment installed, Duke does a walk down w/vendor to ensure location of equipment.

(3) Conclusions:

(4) Date Request(s) Generated:

1. Please provide a copy of the PowerPoint presentation made to Commission staff on July 7, 2014. (Note: No need to provide....staff obtained a copy of the presentation on-site)