INTRODUCTION

In response to Public Act 07-242, "An Act Concerning Electricity and Energy Efficiency", the Connecticut Siting Council (Council) issues this position paper to establish the Council's review in regards to the siting of electric transmission and generating facilities. This policy document was developed to comport with relevant parts of Section 8 of the Public Act which states:

> Not later than September 1, 2007, the Connecticut Siting Council, in consultation with the Emergency Management and Homeland Security Coordinating Council, established pursuant to sections 28-1b of the general statutes, and the Department of Public Utility Control shall initiate a contested case proceeding, in accordance with the provisions of chapter 54 of the general statutes, to investigate energy security with regard to the siting of electric generating facilities and transmission facilities, including consideration of planning, preparedness, response and recovery capabilities. The Connecticut Siting Council may conduct such proceedings in an executive session with sensitive information submitted under a protective order.

Pursuant to legislative intent of the Act, this document will review existing regulations and guidelines regarding security for the siting of electric generating and transmission facilities. Security in this document will only relate to intentional physical threats to a facility. Threats can range from simple trespassing to vandalism to dedicated acts of sabotage. Siting security in this document does not relate to operational, reliability, and maintenance procedures asset connection requirements, or naturally-caused calamities (i.e. hurricanes or ice storms).

EXISTING STANDARDS/GUIDELINES

Presidential Decision Directive 63 "Protecting America's Critical Infrastructures", issued in May 1998, identifies "electricity" as a critical infrastructure. This directive required the U.S. Department of Energy (DOE) to be the lead agency for the protection of critical energy infrastructure (Electricity Sector). The DOE, in turn, designated the North American Electric Reliability Corporation (NERC) as the Electricity Sector Coordinator.

NERC's responsibilities as Sector Coordinator include the following:

- assessment of sector vulnerabilities;
- planning to reduce electric system vulnerabilities;
- development of a system for indentifying and averting attacks;
- development of a notification procedure for sector participants and appropriate government agencies, when an attack is imminent or underway; and
- assist in reconstituting minimum essential electric system capabilities after an attack.

In June 2002, NERC issued "Security Guidelines for the Electricity Sector", Version 1.0, that describe general approaches, considerations, practices, and planning philosophies to be applied in protecting electric system infrastructure. The guidelines are voluntary in nature and were developed to help entities develop policies, procedures, practices and strategies to address issues related to security. Each entity can decide if the particular guideline will be used and to what extent, if any. These guidelines, with subsequent additions and revisions, include the following topics:

- Communications
- Continuity of Business Practices
- Continuity of Operations
- Control System - Business Network Electronic Connectivity
- Control System Cyber Security Incident Response Planning
- Cyber - Access Controls
- Cyber - Intrusion Detection
- Cyber - IT Firewalls
- Cyber - Risk Management
- Emergency Plans
- Employment Background Screening
- Patch Management for Control Systems
- Physical Response
- Physical Security
- Physical Security - Substations
- Protecting Potentially Sensitive Information
- Securing Remote Access to Electronic Control and Protection Systems
- Vulnerability and Risk Assessment

In addition to the aforementioned guideline document, separate voluntary guideline documents were established, as follows;

- Security Guideline for the Electricity Sector -- Threats and Incident Reporting - Version 2, April 2008;
- Security Guideline for the Electricity Sector -- Physical Response - Version 3.0, November 2005; and
- Threat Alert System and Cyber Response Guidelines for the Electricity Sector -- Version 2.0, October 2003.

Although these guidelines are voluntary, mandatory standards were developed as a result of the Energy Policy Act of 2005 that authorized the Federal Energy Regulatory Commission (FERC) to designate a national Electric Reliability Organization (ERO). In July 2006, FERC issued an order certifying NERC as the ERO for the United States.

NERC transformed many existing voluntary policies into mandatory standards to ensure proper design, operation and maintenance of the electric grid to ensure reliability of the system.

Standards were developed to address every aspect of the design, operation, and maintenance of electric infrastructure. Security standards, particularly in the area of cyber security, were developed, including:

Standard CIP-002-1 – Cyber Security – Critical Cyber Asset Identification
Standard CIP-003-1 – Cyber Security – Security Management Controls
Standard CIP-005-1 – Cyber Security- Electronic Security Perimeter(s)
Standard CIP-006-1 – Cyber Security – Physical Security
Standard CIP-007-1 – Cyber Security – Systems Security Management
Standard CIP-008-1 – Cyber Security – Incident Reporting and Response Planning
Standard CIP-009-1 – Cyber Security – Recovery Plans for Critical Cyber Assets
Standard NUC-001-1 – Nuclear Plant Interface Coordination
Standard PRC-001-1 – System Protection Coordination

NERC is continually evaluating and modifying its standards and guidelines to address changing technologies and emerging threats through the Critical Infrastructure Protection Committee (CIPC). The CIPC is comprised of industry experts in the areas of cyber security, physical security, and operational security who coordinate NERC's security initiatives.

Security is addressed in the daily operation of the electricity grid and in future planning of the grid. NERC operates the industry's Electricity Sector Information Sharing and Analysis Center (ESISAC) under the U.S. Department of Homeland Security and Public Safety Canada. ESISAC gathers information about security-related threats and incidents, and communicates it to government authorities.

In addition to NERC, the IEEE (formerly known as the Institute of Electrical and Electronics Engineers, Inc.), a professional organization dedicated to the advancement of technology, issued various guidelines that address different aspects of substation operation, maintenance and security. The security guideline, Standard 1402-2000 – IEEE Guide for Electric Power Substation Physical and Electronic Security, issued in June 2000, addresses security issues related to human intrusion during the construction, operation, and maintenance of electric power supply substations. Methods to deter and mitigate intrusions are discussed.

COMPLIANCE

All bulk power system owners, operators, energy marketers, generators with contracts to sell energy, and local distribution companies must comply with NERC approved operational and reliability standards. In Connecticut, these entities are required to register with NERC through the Northeast Power Coordinating Council (NPCC), the regional organization that ensures reliability to Northeastern North America. Both NERC and the NPCC conduct compliance reviews to enforce the required standards through assessments, audits, evaluations, investigations and analysis of self reporting requirements. Entities that do not meet certain criteria are subject to enforcement action through monetary and non-monetary means.

COUNCIL'S ROLE

Although the task of developing security for the siting of certain aspects and components of electrical infrastructure has been and continues to be examined and addressed by NERC and IEEE through voluntary guidelines and mandatory standards, the Council will consider specific discussion points in regards to security when reviewing a proposed electric generating facility,

transmission facility, or electric substation to ensure the project meets security guidelines and regulatory requirements. Discussing such issues in the application process will improve the Council's scope of review. The Council's expertise in siting of electric generation, transmission, and substation facilities will provide a unique insight for security concerns.

The Council may examine the siting security topics, as set forth in Section 8 of Public Act 07-242, during the application process to ensure they are considered with existing guidelines, standards and other criteria. The topics: Planning, Preparedness, Response and Recovery, may be explored for all proposed electric generating, transmission, and substation facilities;

A. PLANNING

1. Identification

Identify the types of security threats to a facility.
Identify specific vulnerabilities.

2. Facility type/characteristics

Identification of the type and characteristics of the facility.
Description of the facility setting and how the setting affects security concerns.

3. Interdependencies

Examine how the facility is linked to other facilities and systems and potential repercussions from a facility or system interruption.
An examination of how the setting (co-location) of the facility could affect neighboring independent or dependent facilities and systems.

4. Awareness

Examine how vulnerability information is disseminated to employees as well as the public.
Discussion with other industry members or appropriate government agencies to share information regarding threats and countermeasure.

B. PREPAREDNESS

1. Support infrastructure

Examine mechanical systems, physical and non-physical barriers, access control, personnel, and redundant systems required to achieve site security.
Examine types of site monitoring required for manned and unmanned facilities.

2. Personnel

Establishment of a local law enforcement/emergency response liaison.
Mutual Aid Agreements and Emergency Management Assistance Compacts.
Personnel Qualifications and Certifications.
Employee Training.
Simulation and Exercises, including local police, fire, and other emergency response teams.

C. RESPONSE

1. Access to information

Examine notification procedures.
Levels of notification depending on type of security issue.
Proper notification to ensure proper employee or emergency response.

2. Mitigation

Mitigation measures including alternate routing of power, strategically located spares, recovery procedures, redundancy, mutual assistance, mobile backup generation.

D. RECOVERY

1. Recovery Measures

Effective generation re-dispatch plan.
Adequate testing of system or system components prior to restart.
Established communication procedure to ensure restart does not negatively impact other systems or facilities operating under contingency measures.

2. Reporting

Final reporting to determine shortcomings in the security plan and identification of methods of resolution.
Analysis of notification and response actions followed by recommendations to improve response efficiency.

CONCLUSION

The Council recognizes and agrees that electricity is a critical infrastructure as defined by Presidential Decision Directive 63 "Protecting America's Critical Infrastructure". Post September 11, 2001, NERC, as the Electrical Sector Coordinator for DOE and certified by FERC as the ERO, implements and monitors guidelines and standards to ensure proper design, operation, and maintenance of the electric grid. Furthermore, NERC, on a daily basis, operates the industry's Electricity Sector Information Sharing Analysis Center in coordination with the U.S. Department of Homeland Security and Public Safety Canada. The Council understands the complexity of a dynamic system such as the electric grid and accepts and concurs with the layers of oversight that protect it by competent and responsive entities.