



## **NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL**

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731

### **DRAFT Critical Infrastructure Protection Committee Laptop Computer Thefts Scope Document**

#### **Introduction**

The theft of laptop (notebook) computers has occurred with increasing frequency in the electric sector. Numerous incidents (at least six) have been reported in the past two years. This trend will continue unless addressed because the advantages of the portable computers are significant, the cost of the devices continues to come down, more are being issued to employees across the sector, and thieves know the stolen computers are easy to fence and have a high street value. The Critical Infrastructure Protection Committee (CIPC) has decided to address the issue with this situation statement and the attached laptop computer security reference document.

#### **Reasons for Concern**

Theft of laptop computers needs to be reduced for the following reasons:

- 1.** Avoidable — With minimal preventative measures, laptop computer theft can be significantly reduced.
- 2.** Sensitive and critical electric infrastructure information — Increasingly, more sensitive and critical electric infrastructure information is being stored on laptop computers. These include mapping information about key facilities, relay settings for protective systems, customer information, employee information, and SCADA system information. Numerous entities in the electric sector have reported thefts of laptops containing mapping information for their distributions and transmission systems, including substation information. Critical customer information is some times included in the data in the computer. Widespread application of intelligent digital relays has resulted in technicians having the relay settings stored on laptop computers, while some systems are set up for technicians to adjust settings with their laptops.
- 3.** Personal Information — Personal private information is frequently stored on laptop computers. This includes names, addresses, phone numbers, and other valuable information for identity thieves. While not in the electric sector, the theft of a company laptop computer was reported in the November 19, 2005 issue of *The Seattle Post-Intelligencer*. Stored on the computer was personal information concerning 161,000 current and former employees, including names, social security numbers, birth dates, bank names, and account numbers.

4. Economic Loss — The economic loss for each laptop computer can be several thousand dollars, not including the time involved in investigating the theft and the work involved in replacing the device and restoring the information. According to Safeware, the leading computer insurance company, a total of 500,000 laptop computers were lost in the U.S. to theft last year, for a total loss of \$1 billion.

### **Corrective Action**

The CIPC strongly encourages each entity in the industry to strongly emphasize laptop computer security to its employees and to develop strong policies encouraging care and protection of laptop computers. CIPC also recommends the attached reference document be distributed widely across all segments of the industry.