



February 2008

## Theft or Loss of Personally Identifiable Information (PII)

In September 2007, the National Nuclear Security Administration (NNSA) mandated that the loss of PII under the control of NNSA be considered an Incident of Security Concern (IOSC).

### Case

While Jim was on travel, his home was burglarized and his unclassified government laptop was stolen along with some personal valuables. Upon discovering the burglary, Jim's wife called the police department and contacted Jim. He immediately notified his group leader, who reported it to the property custodian and to the organization's security representative. The group leader told the security representative that the computer did not contain classified information. The group leader also indicated that there was no reason for Jim to have any other employee's PII on the computer except his own. However, Jim confirmed that his and his wife's PII were on the government laptop because he had recently worked on the Personnel Security Questionnaire for his clearance. The security representative remembered that reporting requirements for stolen or lost PII had recently changed, so he notified the security inquiry team of the theft of the laptop. The inquiry official confirmed that this matter was a potential IOSC depending on whether the computer contained PII. The matter was categorized as an IOSC and an inquiry was conducted.

### Security Concern

The compromise of an individual's PII can be very serious with ramifications throughout the person's lifetime. DOE and NNSA take seriously their responsibility to safeguard the PII with which they are entrusted. To this end, DOE has required that all PII on government computers taken off-site be encrypted. The confirmed loss of PII under the control of DOE and NNSA is a security incident of the highest order according to NNSA guidance. The loss of PII for up to nine individuals is an Impact Measurement Index 2 (IMI-2) IOSC. Loss of PII for 10 or more individuals is the most severe type of IOSC, an IMI-1.

### Causal Analysis

Jim had a legitimate need to have the government laptop at home. However, he did not need the PII that was on the computer to conduct his work. He had properly protected the PII on the computer with not one, but two, DOE-approved encryptions. DOE mandates that encryption products used to protect DOE information must be certified by FIPS 140-2 (Federal Information Processing Standards). The government computer was reasonably secured in a locked dwelling. Jim was not responsible for the theft. He and his wife are to be commended for rapid reporting to the authorities. The cause of this incident was the criminal act by a person not affiliated with Jim's place of work. Removing the non-essential PII from the computer would not have prevented the theft, but would have prevented a potential unauthorized disclosure of PII.

EVER WONDER WHAT EVENTS  
LEAD UP TO A  
SECURITY INCIDENT?  
CSI CAN UNRAVEL THE  
CLUES.

**CSI:**  
**CONTEMPLATING**  
**SECURITY**  
**INCIDENTS**

EXPLAINING WHAT A  
SECURITY INCIDENT IS  
AND HOW IT UNFOLDS.



## Corrective Actions

A report of stolen property was submitted to remove the laptop from the inventory. Below are some corrective actions Jim's group could implement:

- review all encryption to ensure PII is properly protected by NIST-validated\* products;
- confirm all requirements for off-site use of computers to ensure only the minimum amount of information necessary is taken off-site; and
- conduct a security meeting to brainstorm how to minimize the amount of work that is done remotely.

## Infraction

The incident was not attributed to any DOE or NNSA organization. A security infraction was not issued to Jim, who had properly protected the PII on his government computer and had a legitimate reason to have the computer at home.

## Lessons Learned

Each organization and computer user must:

- carefully review and minimize the need for work to be performed remotely;
- ensure that only the most essential information for that work be loaded onto computers to be taken off-site;
- use a FIPS 140-2 certified product for encryption; and
- whenever possible, avoid having PII on a government-issued computer.

## References

- DOE Office of the Chief Information Officer guidance; <http://cio.energy.gov/policy-guidance/guidance.htm>

## WHAT IS PII?

**Personally Identifiable Information (PII) includes Social Security numbers, place and date of birth, mother's maiden name, and biometric records. If not protected adequately, PII could be used to compromise an individual's identity.**