



JULY 2008

## Classified by Compilation or Association

**Compilation** and **Association** are two circumstances in which separate pieces of otherwise unclassified material can become classified. Compilation occurs when several pieces of unclassified information are combined (not necessarily into one document), resulting in sufficient detail to render the final product classified. Association occurs when two or more different unclassified facts are linked resulting in a classified statement.

### Case

Doug, a Q-cleared employee, joined a group as a manager for a classified project. Doug's group mainly performed classified work and produced daily classified reports. Shortly after his arrival, Doug was asked to develop a comprehensive procedure for the project. Brian, a subcontractor specializing in technical procedures, was hired to assist Doug. Brian emailed Doug asking for a list of the current procedures used. Doug had never compiled such a list but assumed it was a routine administrative task. He pulled from his safe five classified procedures with which he routinely worked. Doug then emailed a list of the unclassified titles of the procedures from his unclassified email account to Brian's off-site business email. Doug, who is not a derivative classifier (DC), knew that emails possibly containing potentially classified information required reviewed for classification prior to distribution. But Doug thought that once deemed "unclassified," the titles could never become classified, so he did not have the email reviewed for classification. Two of the titles created a classified association when combined in the email. Because the email went outside the site's firewall, this incident was categorized as the highest level of security incident based on Department of Energy (DOE) guidelines.

### Security Concern

Unauthorized disclosure is always a potential when classified information is sent via unauthorized channels. The gravity increases when the information is sent outside the laboratory firewall, beyond which control of the information is lost and irretrievable. The lack of security over the Internet and the likelihood of adversarial interception raise concerns. DOE Manual 475.1-1b mandates a DC review of any material "in a subject area that may be classified" prior to transmitting by email. Doug's group had previously stated in a risk categorization memo that all technical work required DC review. Doug saw the memo, but interpreted "technical work" to mean solely measurements, formulas, and "scientific writings". To him, the unclassified title of a document was purely administrative with no potential for being classified regardless of the topic. He was also unaware that unclassified information could be combined to make classified information.

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 .



## **Causal Analysis**

Doug did not seek a DC review for the email because he did not fully understand what comprised technical information. Doug's narrow definition of technical information directly contradicted his organization's definition. Another causal factor was that Doug felt compelled to rush to complete the procedure with clarification or guidance because of Brian's limited-term contract. Finally, Doug had not received formal training on the classified aspects of his job and was not specifically briefed on classified associations. Doug's group's training plan did not require this training.

## **Corrective Actions**

Doug's group implemented additional security awareness training, which highlights email policies and the use of DCs, for all group members.

## **Infraction**

Doug received a security infraction for failing to have a DC review his email before sending it. He also received verbal counseling.

### ***ISSM Focus: Step 2 – Analyze the security risk.***

Doug's incorrect assumption of what constitutes classified information prevented him from identifying the security threat prior to sending the email. Given that Doug was new in his position and had the task of creating a new process, it was all the more important that he implement the five-step ISSM process.

***Work securely.***

***Think ISSM before, while, and after  
you do your work.***

## **Lessons Learned**

- Before distributing information that has been compiled or associated from different classified or potentially classified sources, consider whether its classification has changed. Ask a DC to review the content.
- Do not let a deadline, or in this case another worker's limited-term contract, interfere with your responsibilities to protect classified information.
- If you are unsure about a new process, stop and think if there are classification issues involved.

*Get help if you need it.*