Office of Security Enforcement
Classified Information Security Breakout Sessions
March 27, 2012

SCENARIO OBJECTIVES

PART I

Each of the four scenarios has two parts; **Part I** objective – Determine the appropriate Significance Level Category (**A** or **B**) and Type (Security Interest (**SI**), Management Interest (**MI**) or Procedural Interest (**PI**)), using the provided *DOE O 470.4B, Attachment 5, Section 1, Incident Identification and Reporting Requirements.* The determination of the Significance Level Category and Type should be based on the facts as stated in each scenario.

- Hint: **Category A** incidents meet a designated level of significance relative to the potential impact on the Department and/or national security and requires notification to DOE/NNSA cognizant security office (CSO). Category A incidents must be reported in the Safeguards and Security Information Management System (SSIMS). **Category B** incidents are less significant and do not meet Category A incident criteria and require notification to the contractor CSO. Category B incidents are not required to be reported in SSIMS; however if not reported in SSIMS, Category B incidents must be maintained in a local tracking system.

- Note: Only two incident types involve the protection and control of classified information: (1) **Category A – SI** incidents involve the loss, theft, compromise or suspected compromise of any classified matter, and (2) **Category B – PI** incidents do not result in the loss, theft, compromise or suspected compromise of classified assets, and are supported by documented evidence that suggest compromise did not occur or the likelihood was remote.

- Note: Two flowcharts have also been provided to aid you in determining the appropriate Significance Level Category and Type.

PART II

Part II objective – Based on the information provided for each scenario, determine which, if any, potential noncompliances would be associated with the circumstances of each scenario, using the provided list of *Specific Program Requirements.*

Hint: For each scenario, there may be one or more noncompliant conditions that apply (e.g., Security Program Planning; Issues Management; and Classified Cyber Security.

***** *THIS PAGE INTENTIONALLY LEFT BLANK* *****

Office of Security Enforcement
Classified Information Security Breakout Sessions – Part I
March 27, 2012

IOSC POLICY REQUIREMENTS FOR INCIDENT CATEGORIZATION

1. INCIDENT IDENTIFICATION AND CATEGORIZATION. DOE uses a graded approach for the identification and categorization of IOSCs. This approach provides a framework for the requirements of reporting timelines and the level of detail for inquiries into, and root cause analysis of, specific security incidents. By establishing a graded approach, line management can effectively allocate the resources necessary to implement this policy.

   a. All IOSCs must be categorized by significance level and type. As Table 1 illustrates, there are two levels of significance and three types of incidents.

Table 1. Significance Levels and Incident Types

SIGNIFICANCE LEVEL CATEGORY	
A	B
INCIDENT TYPE	
Security Interest (SI)	Security Interest (SI)
Management Interest (MI)	Management Interest (MI)
Procedural Interest (PI)	Procedural Interest (PI)

   b. Incident Significance Level Categories.

      (1) Category A incidents, which meet a designated level of significance relative to the potential impact on the Department and/or national security, require the notification of the DOE/NNSA CSO and the contractor CSO. The involvement of the DOE/NNSA CSO for Category A incidents is imperative for assessing impacts, coordinating with external agencies, and/or notifying senior management.

      (2) Category B incidents, which do not meet the Category A criteria, are managed and resolved by the contractor CSO; however, this does not preclude the DOE/NNSA CSO from exercising its oversight responsibilities. The monitoring of Category B incidents by the contractor CSO is essential as it allows management to proactively address reoccurring incidents, thereby minimizing the occurrence of potentially more significant incidents.

   c. Incident Types.

      (1) Security Interest (SI). This type of incident involves the loss, theft, compromise, or suspected compromise of Departmental assets.

(2) Management Interest (MI). This type of incident does not necessarily involve Departmental assets but is a unique type of incident that may have potential undesirable impacts. MI incidents therefore warrant management notification. MI incidents differ from SI and Procedural Interest (PI) incidents in that the emphasis is on notification; therefore, MI incidents do not require formal inquiry, closure, etc.

(3) Procedural Interest (PI). This type of incident is associated with the failure to adhere to security procedures, and all evidence surrounding the incident suggests the asset was not compromised or the likelihood of compromise is remote.

d. Incident Criteria. Based on the three types of incidents, the following provides a general framework for distinguishing between Category A and B incidents.

(1) SI.

a) Category A SI incidents involve the following assets:

1. SNM and nuclear material (note that "Loss" does not include quantities that are within established shipping, processing, and inventory limits);

2. All classified matter;

3. As one involving quantities of radiological, chemical, and/or biological materials that if misused could endanger the public;

4. Security key or keycard based on the significance of the asset being protected and the degree of access provided by the key or keycard (e.g., direct access versus access impeded by other layers/measures);

5. Protective force firearms, ammunition, explosives, and equipment per the reporting requirements in DOE M 470.4-3A, *Contractor Protective Force,* dated 11-05-06, and other equipment documented in the site IOSC program plan;

6. DOE security badge determined to be the target of the theft;

7. Matter of a foreign government that requires reporting based on established agreements and required protocols; or

8. Other assets determined by the DOE/NNSA CSO and/or contractor CSO.

b) Category B SI incidents involve the following assets:

1. Official Use Only (Ex 2); Official Use Only/Export Controlled Information (Ex 2 or 3); Unclassified Controlled Nuclear Information; Naval Nuclear Propulsion Information; and

2. Other assets as determined by the DOE/NNSA CSO and/or contractor CSO.

(2) MI.

a) Category A MI incidents are significant enough to warrant notification to the DOE/NNSA CSO. Examples include work stoppages, arrest of an employee enrolled in a human reliability program, etc. Incidents constituting or determined to be a Category A MI must be specified in the IOSC program plan.

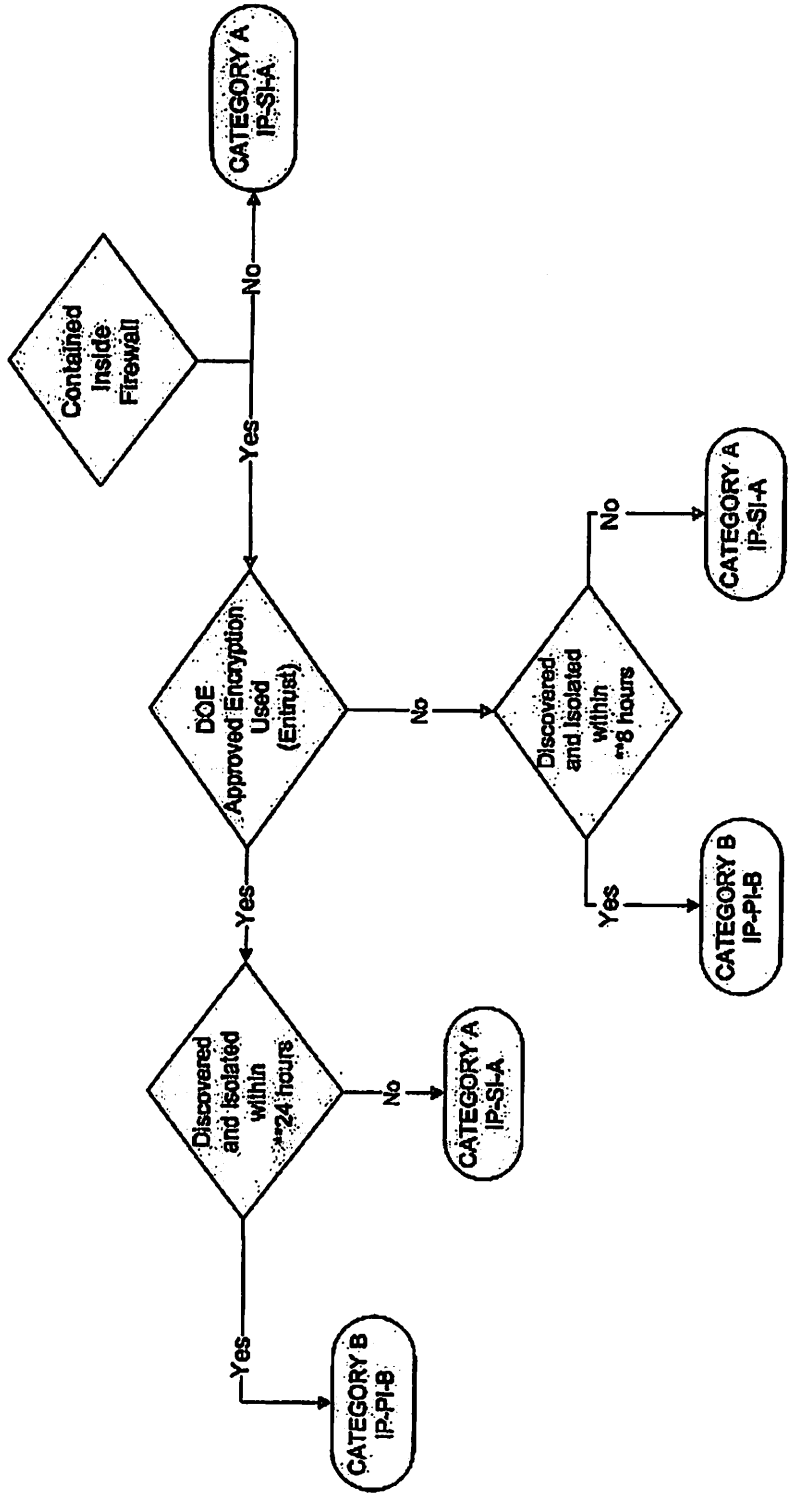
b) Category B MI incidents require notification to the contractor CSO. Incidents constituting or determined to be a Category B MI must be specified in the IOSC program plan.

(3) PI.

a) Category A PI incidents are associated with the failure to adhere to security procedures and warrant notification to the DOE/NNSA CSO. An example of a Category A PI incident is an unauthorized discharge and other incidents determined by the DOE/NNSA CSO and/or Contractor CSO.

b) Category B PI incidents do not result in the loss, theft, compromise or suspected compromise of the asset. These incidents are supported by evidence that suggest the likelihood of compromise is remote or that compromise did not occur. An example of a Category B PI incident would be the improper handling, and/or storage of classified matter, where the supporting evidence suggests compromise did not occur or the likelihood was remote.

***** *THIS PAGE INTENTIONALLY LEFT BLANK* *****

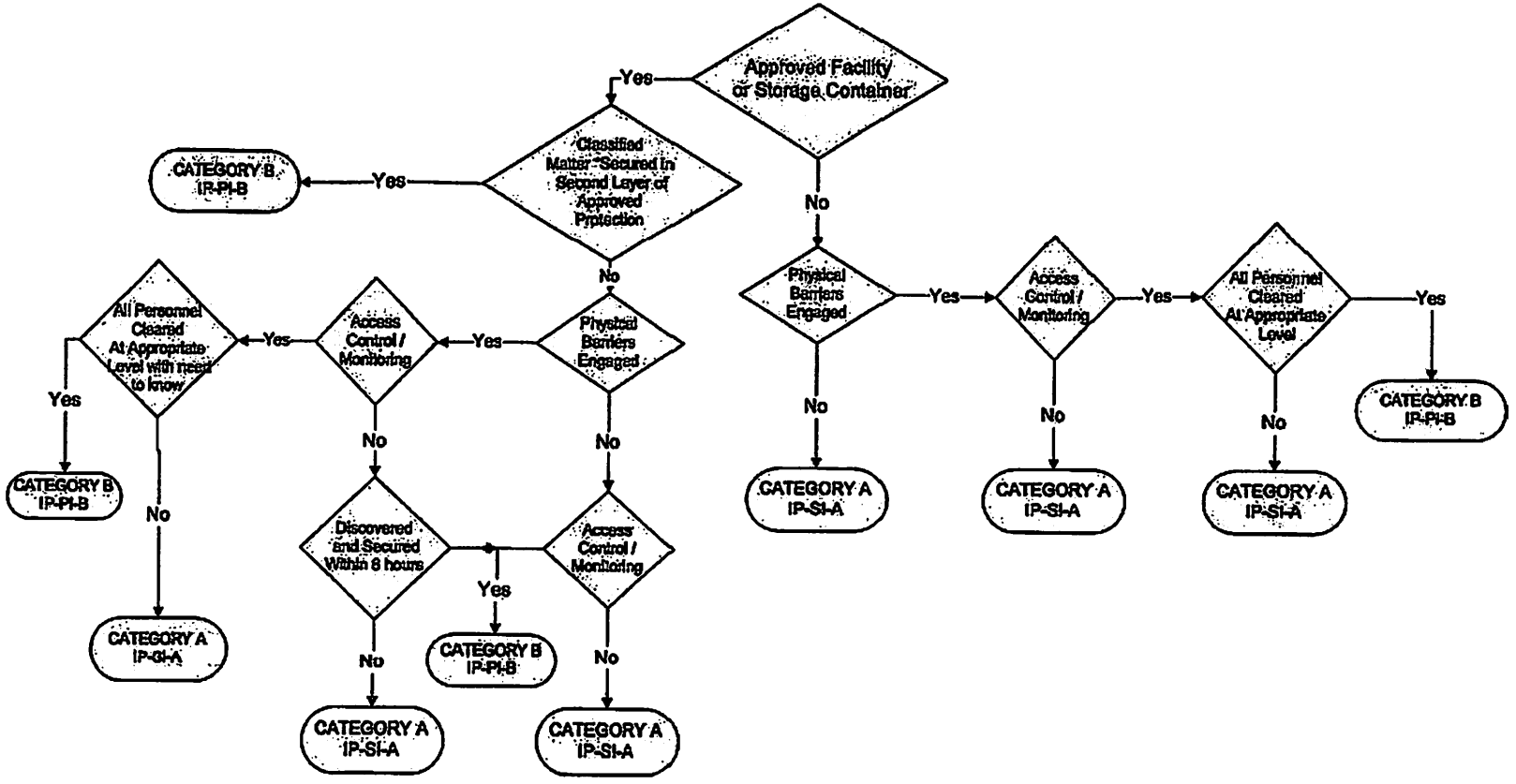


** Within 8 hours from occurrence: System Taken Off-Line; Appropriately Stored Pending Sanitization; Affected Systems Identified

Note: When selecting category B, ensure that documented evidence has been obtained that rules out or mitigates the likelihood of compromise

Figure 4. Unauthorized Network-Based Transmission of Information

***** *THIS PAGE INTENTIONALLY LEFT BLANK* *****



Second Layer of Protection: i.e., LA door unsecure, however all classified matter is secured in approved repositories.
Physical Barriers Engaged: i.e., locked door, locked repository, no evidence of entry through windows, walls, etc.
Access Control / Monitoring: i.e., cipher lock or card reader records; visual surveillance via video camera or personnel; volumetric sensors.

Note: When selecting category B, ensure that documented evidence has been obtained that rules out or mitigates the likelihood of compromise

Figure 1. Improper Storage: Classified Matter

***** *THIS PAGE INTENTIONALLY LEFT BLANK* *****

Office of Security Enforcement
Classified Information Security Breakout Sessions – Part II
March 27, 2012

SPECIFIC PROGRAM REQUIREMENTS

1) **Security program planning.**

(a) Contractors shall develop security plans to ensure classified information is protected from theft, espionage, unauthorized access, compromise, and other acts that may have an adverse impact on national security.
(b) Security plans and procedures shall provide a description of the implementation of classified information protection requirements and strategies, and provide detailed information on the assignment of roles, responsibilities, and authorities, as well as the allocation of resources.
(c) Security plans shall include system effectiveness determinations for the prevention and/or timely detection of the loss of classified information based on the status of performance indicators, such as results of inquiries, performance tests, assessments, and evaluations of personnel qualifications and training.
(d) Security plans shall be reviewed to ensure that plans are current and reflect the actual operating conditions and changes shall be appropriately approved.

2) **Performance assurance.**

(a) Performance assurance programs shall be developed, managed, and implemented to validate the protection of classified information security interests and activities.
(b) Performance assurance programs shall demonstrate effectiveness by systematically evaluating the protection and control provided to classified information.
(c) Performance assurance testing shall be documented to include a narrative description of the test activity and analysis of test results.

3) **Self-assessment.**

(a) Self-assessments shall provide assurance to the Secretary and Cognizant Secretarial Officer that classified information is protected at the required levels.
(b) Self-assessments shall provide a basis for line management to make decisions regarding classified information security program implementation activities, including allocation of resources, acceptance of risk, and mitigation of vulnerabilities.
(c) Compliance-and performance-based self-assessments shall be capable of identifying noncompliances with classified information security requirements associated with programs and activities designed to protect and control classified information.
(d) The contractor shall evaluate their self-assessment processes and incorporate any identified process improvements, including lessons learned, to ensure effective performance.

4) **Issues management.**

(a) Corrective action plans shall be developed and implemented for all noncompliances associated with classified information security requirements.
(b) Corrective actions shall be based on documented root cause analyses and risk assessments to prevent the likelihood of recurrence.
(c) Corrective actions shall be tracked and updated until completed, validated, closed, and verified for effectiveness and sustainability.

5) **Security training and awareness.**

(a) Contractors shall establish training programs that ensure personnel are trained to a level of proficiency and competence that ensures they are qualified to perform assigned tasks and/or responsibilities related to the protection and control of classified information.
(b) Contractors shall provide awareness briefings to ensure individuals are informed of their classified information security responsibilities.

6) **Classification.**

(a) Contractors shall ensure that classification guidance is identified for all work performed in a classified subject area that may generate classified documents or material.
(b) Contractors shall ensure a classification review is obtained if there are any questions regarding the classification of any draft document or working paper.
(c) Contractors shall ensure personnel are trained to perform classification reviews and determinations in accordance with appropriate classification guides.

7) **Classified matter protection and control.**

(a) Contractors shall ensure that prior to classification review, the information shall be protected at the highest potential classification level and category.
(b) Contractors shall protect and control classified information that is generated, received, transmitted, used, stored, reproduced, permanently buried or to be destroyed to prevent loss, compromise or unauthorized disclosure to anyone without the appropriate access authorization or need-to-know for that information.
(c) All classified information shall be marked in accordance with current requirements. These markings shall include sufficient information to allow individuals using/handling classified information to provide the appropriate level of protection and control.
(d) Contractors shall establish an integrated security system to prevent, detect, or deter unauthorized access, modification, or loss and/or the unauthorized removal of classified information from a site or facility.

8) **Classified cyber security.**

(a) Information systems used to process classified information shall be approved (i.e., certified and accredited) in accordance with current requirements to ensure the establishment of adequate and effective security controls.
(b) Classified processing shall take place in a DOE approved location.

9) **Incidents of security concern.**

(a) Contractors shall accurately notify DOE, investigate, and report incidents of security concern involving classified information security requirements. An initial report shall be filed within five (5) calendar days, or within the time period established by applicable DOE rule or order, of the date of discovery.
(b) Contractors shall establish and maintain complete and accurate records for all incidents of security concern involving classified information security requirements.
(c) Contractors shall analyze incidents of security concern data for trends and lessons learned.

***** *THIS PAGE INTENTIONALLY LEFT BLANK* *****

Office of Security Enforcement
Classified Information Security Breakout Session Scenarios 1 - 4
March 27, 2012

***** *THIS PAGE INTENTIONALLY LEFT BLANK* *****

Office of Security Enforcement
Classified Information Security Breakout Session Scenarios
March 27, 2012

SCENARIO 1

On January 1, 2012, Headquarters sent an unclassified e-mail to Site X containing a call for white papers regarding a number of topics related to classified subject areas. On the same day, the recipient of the unclassified e-mail, Site X Program Manager, (Q cleared), forwarded the unclassified e-mail to six employees (all Q cleared), within the Division. One of the employee's began to research background information via the Internet for one of the white paper topics, hereinafter referred to as, subject topic.

On January 17, the Site X employee sent a zip file, via the Site's unclassified network, with all the background information that was researched for the subject topic to three outside collaborators (all uncleared), at the Y Institute. This same employee also sent an e-mail, via the Site's unclassified network, to these collaborators regarding the request for white papers Site X had received.

On January 24, one of the collaborators from the Y Institute sent an e-mail with a draft white paper attached titled, "Site X Subject Topic" to the Site X employee and the two other collaborators. On January 27, the Site X employee sent an e-mail, via the Site's unclassified network, with the draft white paper attached to the Site X Program Manager.

On January 28, the Site X employee finalized the draft white paper and sent an e-mail, via the Site's unclassified network, with the final white paper attached (i.e., "Site X Subject Topic"), to the Site X Program Manager. That same day, the Site X Program Manager sent an e-mail, via the Site's unclassified network, with the "Site X Subject Topic" white paper and other white papers to Headquarters, and copied nine other Division employees; (six Q cleared, 3 uncleared). Two of the uncleared recipients were foreign national students from a sensitive country. In addition, the Site X employee sent the final white paper to the collaborators at the Y Institute.

On February 4, Headquarters called the Site X Program Manager to indicate a classification concern. Based on this concern from Headquarters, the white paper, "Site X Subject Topic" was reviewed by the Site's classification officer, and determined to be classified at the Secret/Restricted Data level.

During the inquiry process, it was found that a security self-assessment of this Division had just been conducted. The self-assessment team relied on prior knowledge that this Division has not been involved with classified work for years, and limited the assessment scope to only legacy classified holdings. In addition, the Site X employees involved in this incident stated to the inquiry official that they had not been appropriately trained in working with classified information.

ANSWER:

Significance Level Category (**A** or **B**) _____ Type (**SI** or **PI**) _____

Potential Noncompliances (Specific Program Requirements)

_____
_____
_____
_____
_____
_____

Office of Security Enforcement
Classified Information Security Breakout Session Scenarios
March 27, 2012

SCENARIO 2

An employee (Q cleared) of Site X prepared an e-mail dealing with a classified subject area on an unclassified information system, believing that the information in the e-mail was not classified. This employee, who is not a derivative classifier (DC), sent the e-mail, via the Site's unclassified network, to 15 other Site X employees (all Q cleared working on the same project).

Immediately after receiving the e-mail, one of the recipients advised the employee who originated the e-mail to have it reviewed by a DC. Based on the concern raised, this employee immediately sent the e-mail, via the Site's unclassified network, to the DC for a classification review.

Within minutes of receiving the e-mail, the DC reviewed the content and notified the originator of the e-mail to discuss suggested changes. Based on the suggestions from the DC, the employee who originated the e-mail made the suggested changes and resent the e-mail to the same 15 Site X employees.

The recipient, who raised a concern with the first e-mail, had another concern with the second e-mail. This recipient took both the original e-mail and the revised e-mail to the Site's classification officer for a classification review. The classification officer discussed both e-mails with the originator, and the DC who reviewed the original e-mail and provided the suggested changes for the second e-mail.

It was determined by the classification officer that the original e-mail contained information classified at the Confidential/Restricted Data level, and the second e-mail, which included the suggested changes by the reviewing DC, contained information at the Secret/Restricted Data level. Based on discussions with the DC who originally reviewed the e-mail, it was determined that the DC failed to recognize the classification concerns that originally existed and did not consult any classification guides when giving classification advice. This resulted in the second e-mail being sent, containing classified information at a higher classification level.

It was found that the original e-mail was sent at 7:00 a.m., and the second e-mail was sent at 11:00 a.m. on the same day. By 2:45 p.m. that day, all systems affected by both e-mails were identified and appropriately sanitized.

ANSWER:

Significance Level Category (**A** or **B**) _____ Type (**SI** or **PI**) _____

Potential Noncompliances (Specific Program Requirements)

_____
_____
_____
_____
_____

Office of Security Enforcement
Classified Information Security Breakout Session Scenarios
March 27, 2012

SCENARIO 3

An employee, (Q cleared) at Site X was undergoing a random polygraph examination and as a result, the employee recalled a security incident involving the protection and control of classified matter that needed to be reported. The employee explained that a security incident had occurred approximately three years ago, but it was never reported as an incident of security concern. The employee also reported five additional security incidents that should have been reported, but they did not involve classified information.

The incident involving the protection and control of classified information took place while attending a meeting at another facility, Site Y. The employee was attending two meetings while at Site Y, (each meeting was on a separate day). The first meeting was held in a Sensitive Compartmented Information Facility (SCIF) at Site Y. The employee explained that documents were distributed as handouts during the meeting. When the meeting concluded, the employee placed all the distributed documents in a briefcase and left the SCIF.

After leaving Site Y for the day, the employee returned to the hotel, dropped off the briefcase, and left the hotel for dinner and sight-seeing (approximately 6 hrs). The following morning, the employee returned to Site Y for another meeting that took place in the same SCIF. The employee opened the briefcase and determined that some of the documents taken the day before were classified.

Without mentioning anything, the employee separated the classified documents from the unclassified documents and placed them all on the table in the meeting room. At the conclusion of the meeting, the employee left the SCIF and Site Y to return home. The employee did not report what had happened to either Site Y, or Site X security incident program offices. Based on the topics of the meetings, it was determined that the classified information the employee removed and failed to properly protect and control from Site Y was classified at the Secret, No Foreign level.

ANSWER:

Significance Level Category (**A** or **B**) _____ Type (**SI** or **PI**) _____

Potential Noncompliances (Specific Program Requirements)

_____
_____
_____
_____
_____
_____

Office of Security Enforcement
Classified Information Security Breakout Session Scenarios
March 27, 2012

SCENARIO 4

Employee A (Q cleared) at Site X was originating a document (Doc A) dealing with a classified subject matter and wanted the document to be unclassified – Official Use Only (OUO) so the document could be used as a source-document and openly shared with other Site X employees. Employee A, who is not a derivative classifier (DC), developed the original document on an approved classified information system to avoid potential issues with classification before it could be reviewed by a DC.

Upon completion of Doc A, employee A took the document to the classification office for review. The DC determined that the document was OUO. Based on the classification review, employee A e-mailed Doc A, using Entrust encryption via the Site's unclassified network, to other Q cleared Site X employee's working on the project.

Another Site X employee (employee B), who is working on a different but related project, needed some information from Doc A. Employee B was directed to Doc A located on the classified network and was told that the document had been reviewed by a DC and determined to be OUO. Employee B took information from Doc A and created another document (Doc B) using an unclassified information system. Because Employee B used information from Doc A, which had been reviewed by a DC and determined to be OUO, and the additional information incorporated was from unclassified sources, employee B did not have Doc B reviewed for classification.

Employee B e-mailed Doc B, using approved Site X encryption via the Site's unclassified network, to other Q cleared Site X employee's working on the project. One of the recipients of Doc B is a DC and has classification authority for the subject matter of Doc B. The DC review determined Doc B was classified at the Secret/Restricted Data level. The classification issue was determined to be a compilation.

Within 24 hours of Doc A and Doc B being e-mailed via the unclassified network using Entrust encryption, all affected information systems were identified and appropriately sanitized.

ANSWER:

Significance Level Category (**A** or **B**) _____ Type (**SI** or **PI**) _____

Potential Noncompliances (Specific Program Requirements)

_____
_____
_____
_____
_____
_____

******END******