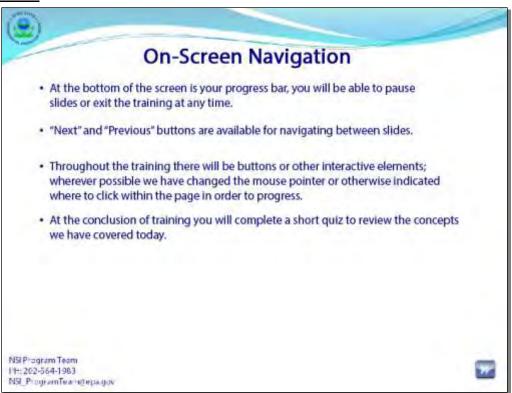
Slide1

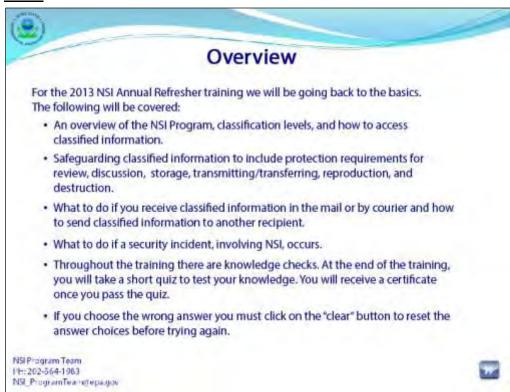


Slide2

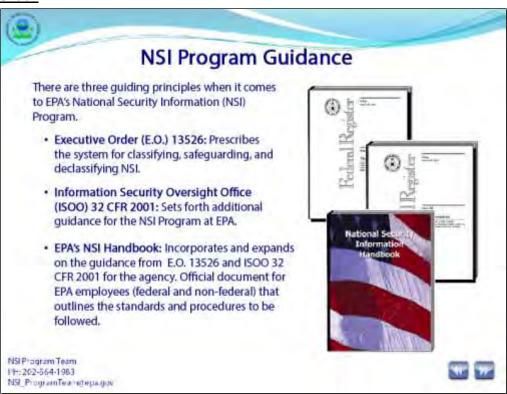


, 1 of 27

Slide3

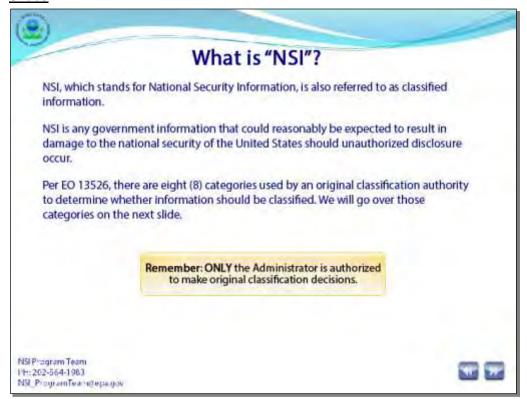


Slide4



, 2 of 27

Slide5

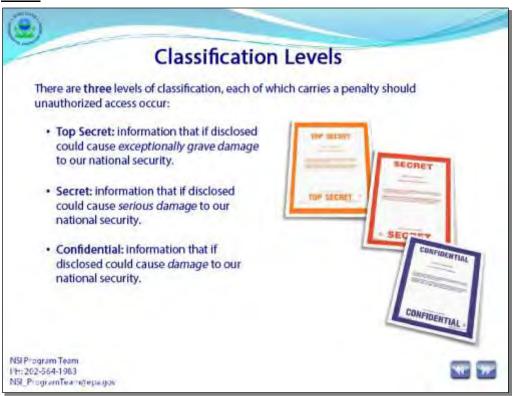


Slide6

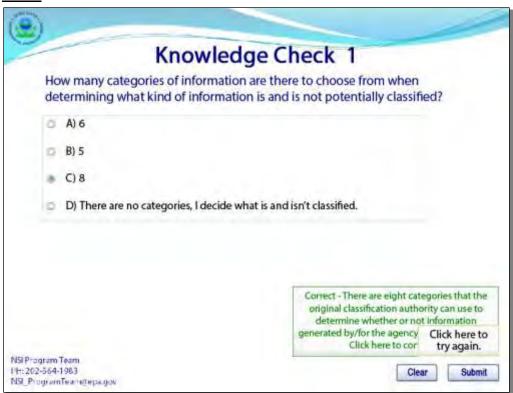


3 of 27

Slide7

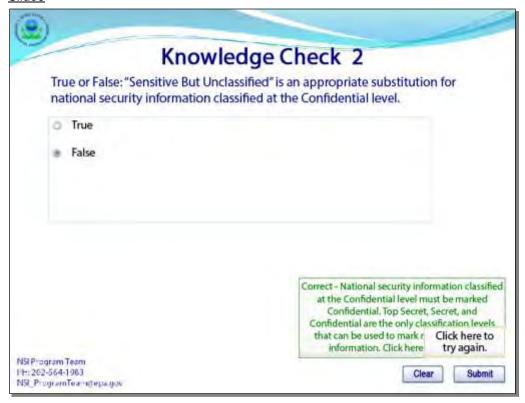


Slide8

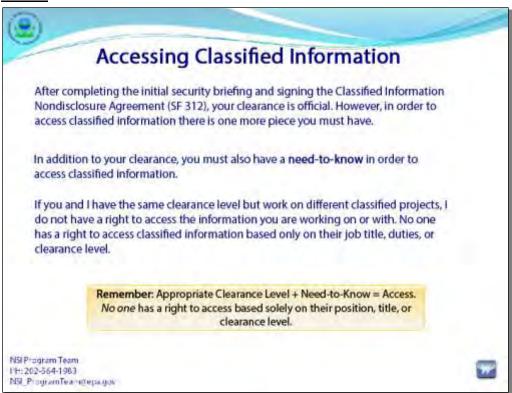


, 4 of 27

Slide9



Slide10



, 5 of 27

Slide11



All work that involves classified information *must* take place in a secure area. Let's discuss the types of activities that may involve classified information first and then we will discuss secure areas in more depth.

Activities that may involve classified information are:

- · Discussion and/or Review.
- Storage in GSA approved security containers.
- Processing only on approved classified computers.
- · Reproduction.
- · Destruction.

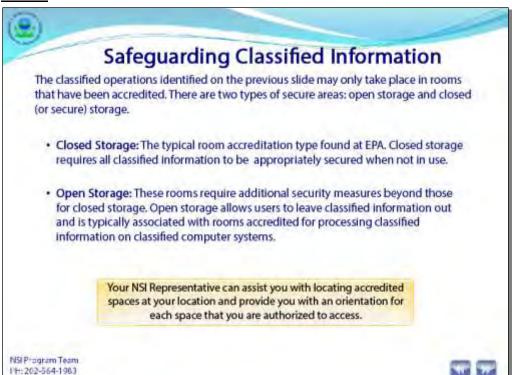
NSI Program Team I'H: 202-564-1983 NSI_ProgramTeam@epa.gov

NSI ProgramTea intepagov



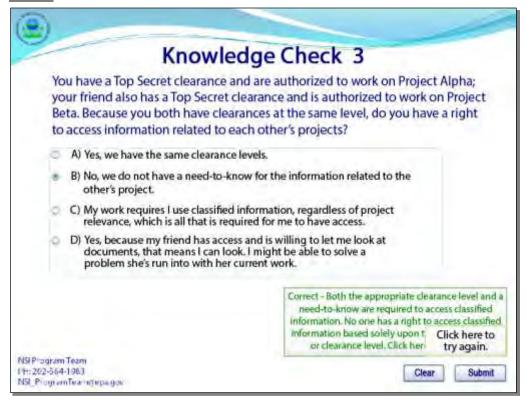


Slide12

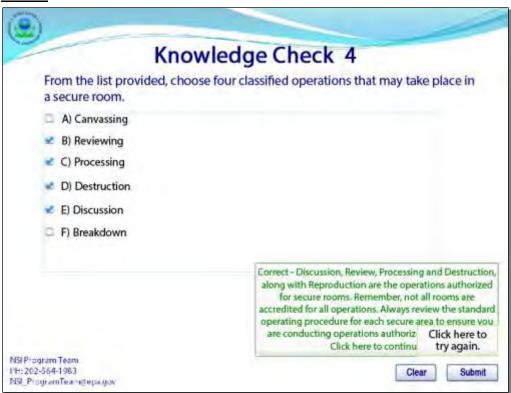


, 6 of 27

Slide13

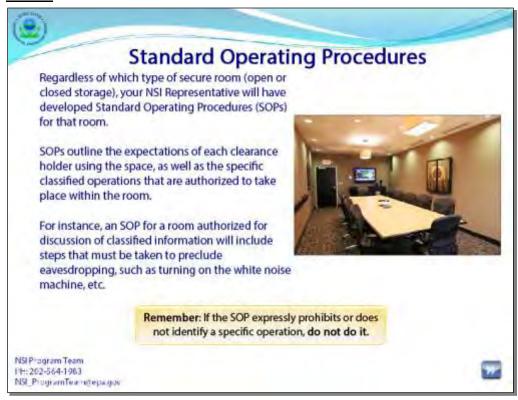


Slide14

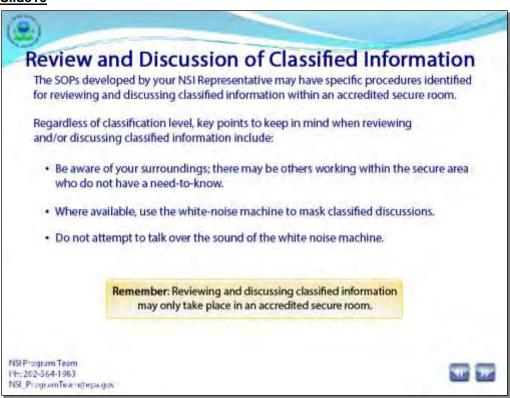


7 of 27

Slide15



Slide16

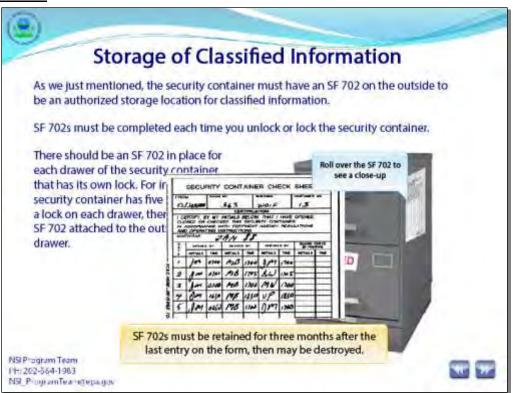


, 8 of 27

Slide17

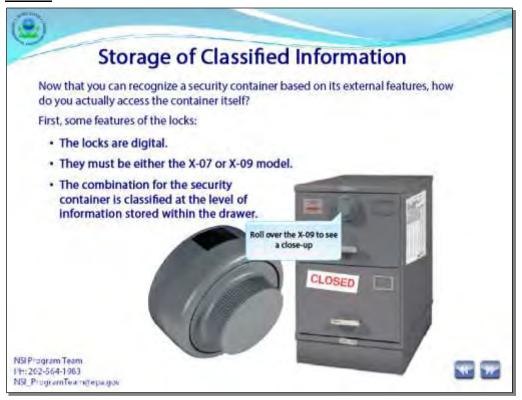


Slide18

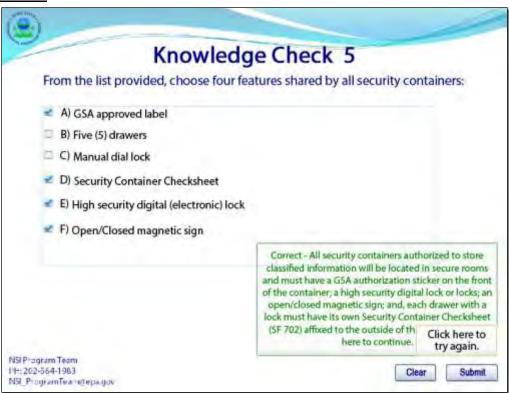


, 9 of 27

Slide19

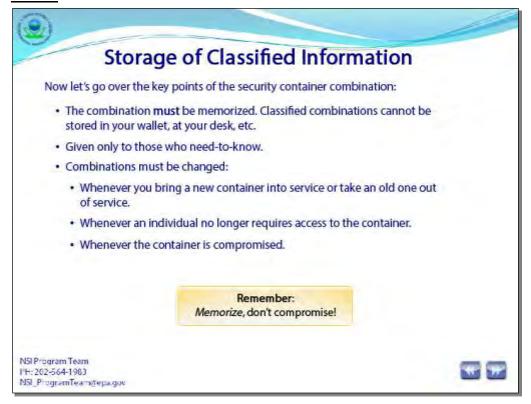


Slide20

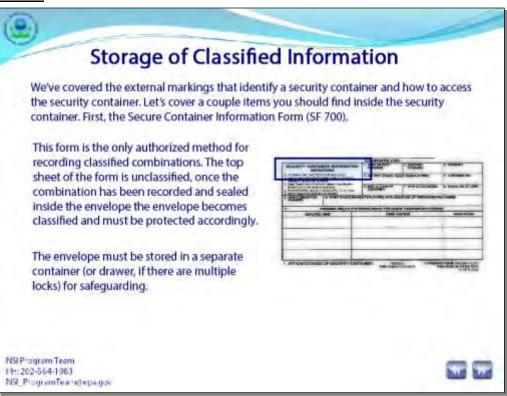


, 10 of 27

Slide21

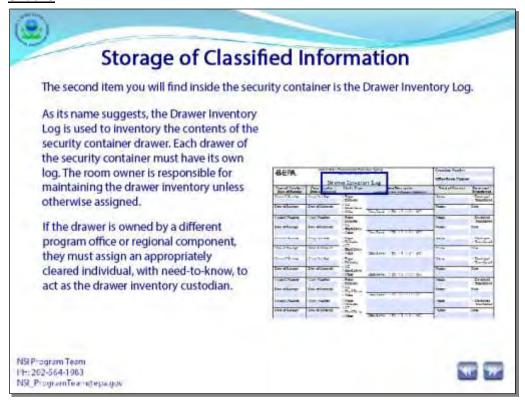


Slide22

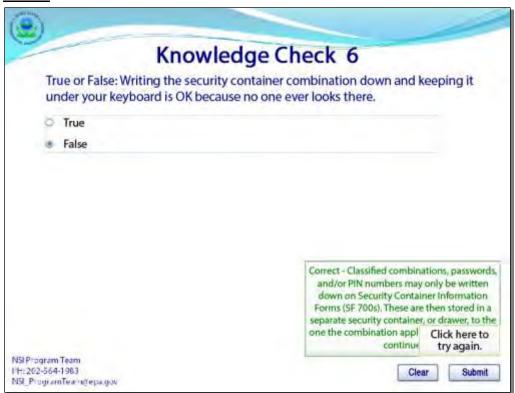


, 11 of 27

Slide23

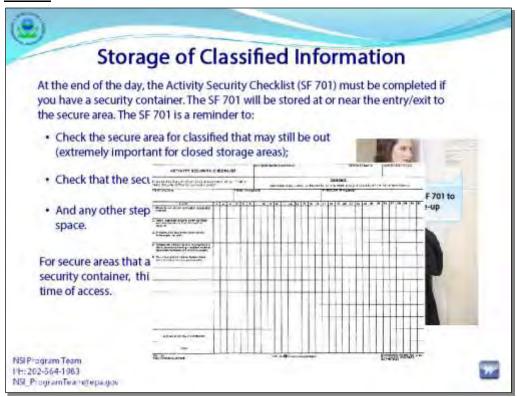


Slide24



, 12 of 27

Slide25



Slide26



, 13 of 27

Slide27

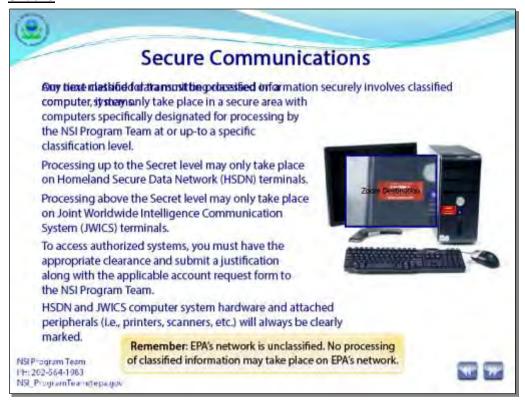


Slide28

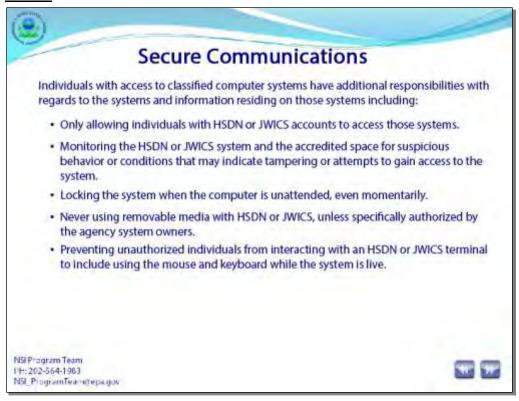


, 14 of 27

Slide29



Slide30



, 15 of 27

Slide31



Secure Communications

In addition to protecting the systems, as an authorized user you must also protect your access credentials. The following steps are recommended:

- Create a strong password and protect it at the level of the system that you have
 - Strong passwords include the use of upper and lower case letters, numbers, and special characters.
 - Phrases that use a mixture of characters are stronger than single words. (i.e., 110v3\$3curlty is stronger than \$3curlty)
- Do not reuse passwords from unclassified systems or programs on a classified system.
- Passwords may be written on an SF 700 and stored in an approved GSA security container at the appropriate classification level.
- Do not allow anyone to view classified information available on HSDN or JWICS without an appropriate clearance and a need to know for the level of the information.

NSI Pragram Team PH: 202-564-1983 NSI ProgramTea intepagov





Slide32



Secure Communications

As an authorized user, the following guidelines must be followed when printing documents. from HSDN or JWICS:

- Ensure all classified documents are cleared from the printer's "queue" before logging off or shutting down the computer. If there are jobs pending in the queue they must be completed before logging off or shutting down.
- · Do not leave classified documents on the printer.
- Ensure all printed documents have the appropriate classified coversheet attached to the front of the document and are placed in a GSA-approved security container if they will be retained; you must also update the Drawer Inventory Log.
- For documents printed from JWICS that are classified as Top Secret or that contain Sensitive Compartmented Information, an EPA Form 1350-2 must be completed to document destruction, prior to shredding the material. A witness must be present for destruction of these documents.
 - Documents classified at Secret and below do not require an EPA Form 1350-2 be completed specifically to document destruction.

If you have questions regarding classified computer systems, please contact your NSI Representative or the NSI Program Team.



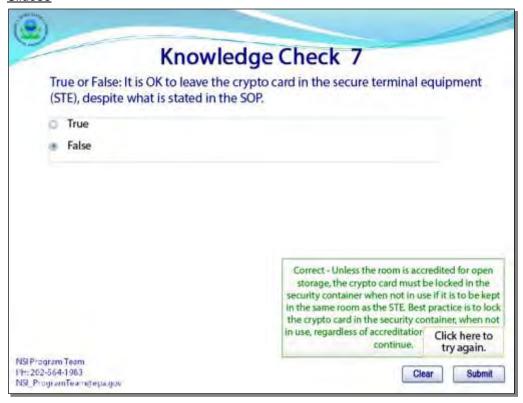


NSI Pragram Team PH: 202-564-1983

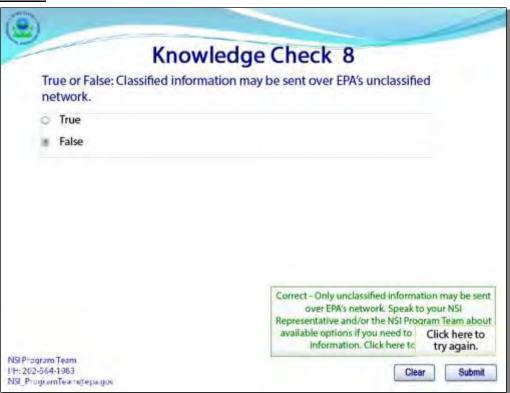
NSI_ProgramTeammepa.gov

16 of 27

Slide33

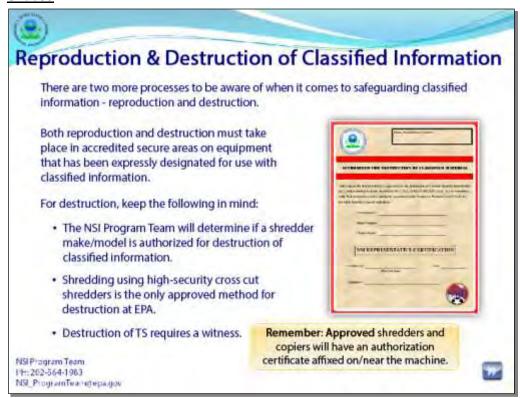


Slide34

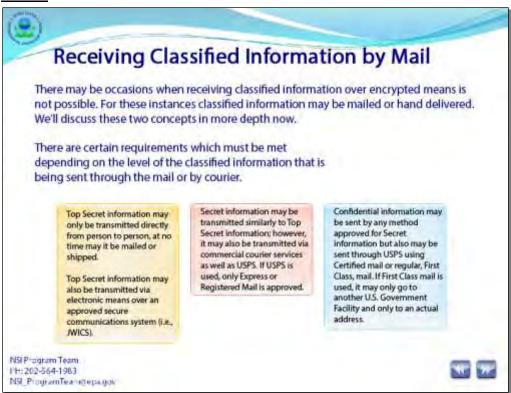


, 17 of 27

Slide35

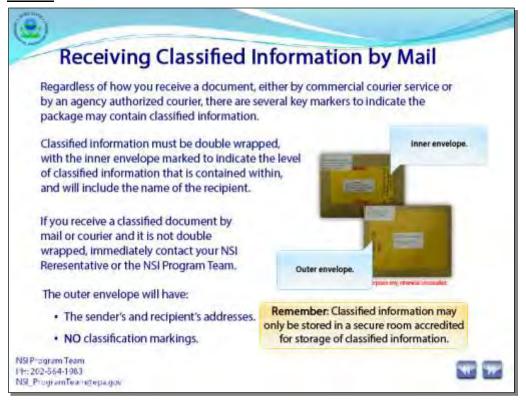


Slide36

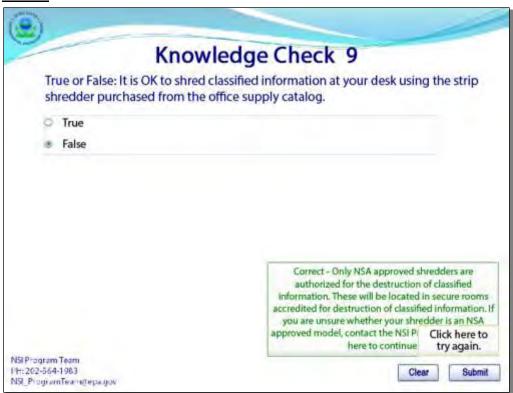


, 18 of 27

Slide37

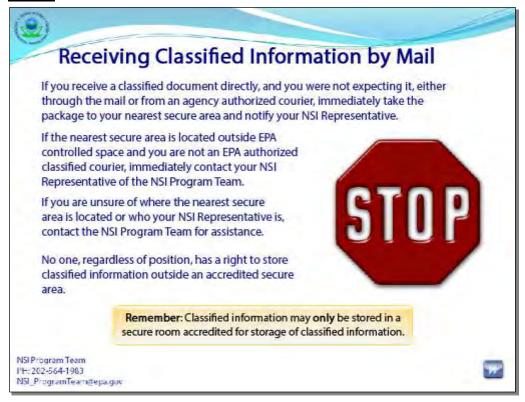


Slide38



, 19 of 27

Slide39



Slide40



, 20 of 27

Slide41

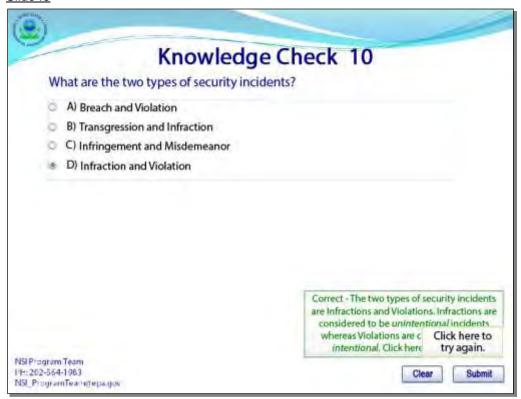


Slide42

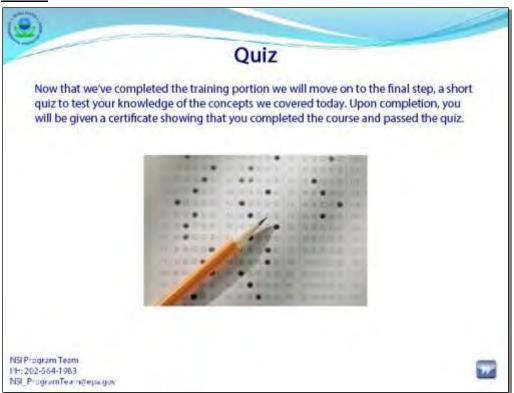


, 21 of 27

Slide43

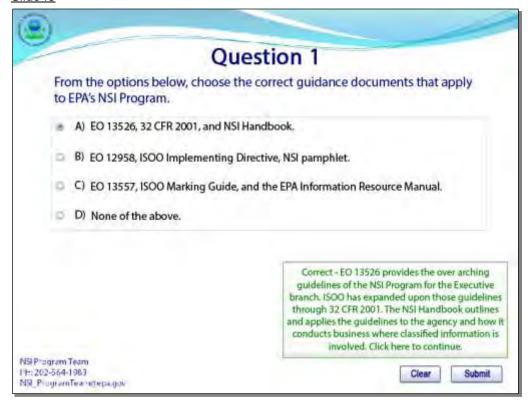


Slide44

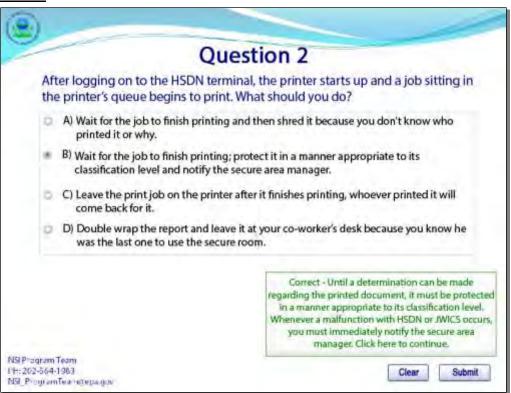


, 22 of 27

Slide45

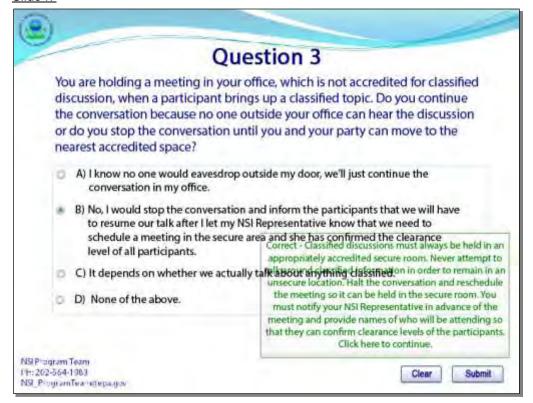


Slide46

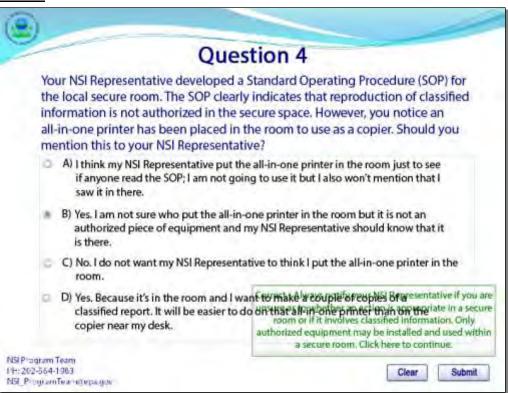


, 23 of 27

Slide47

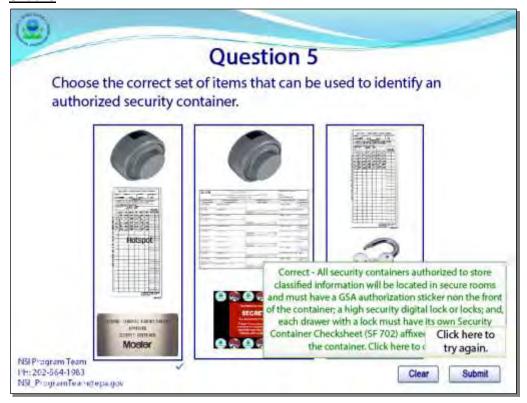


Slide48

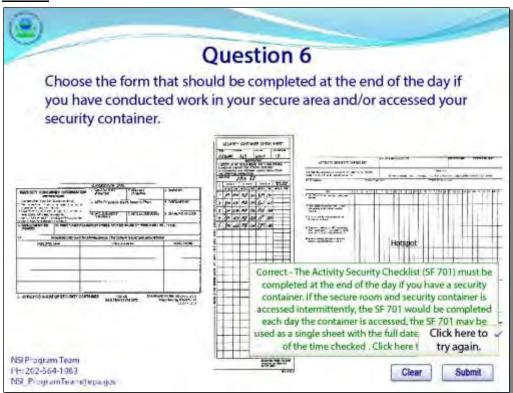


, 24 of 27

Slide49

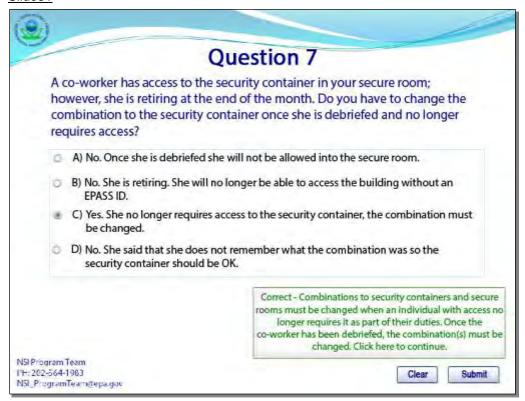


Slide50

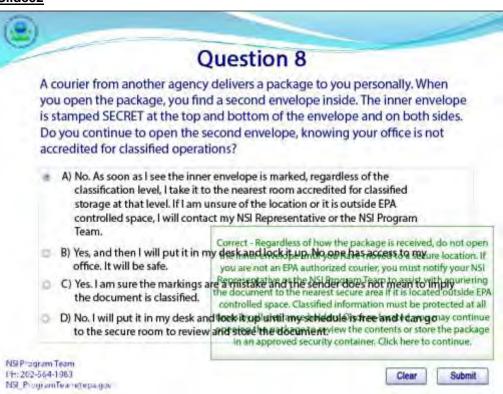


, 25 of 27

Slide51

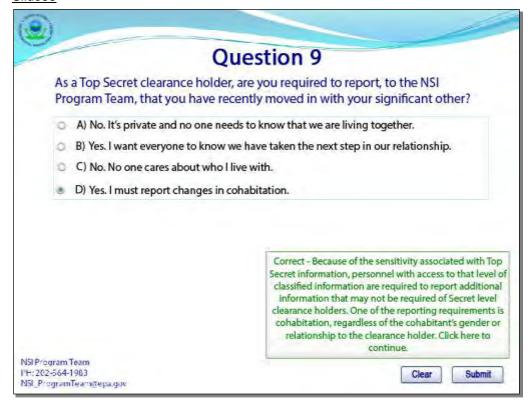


Slide52

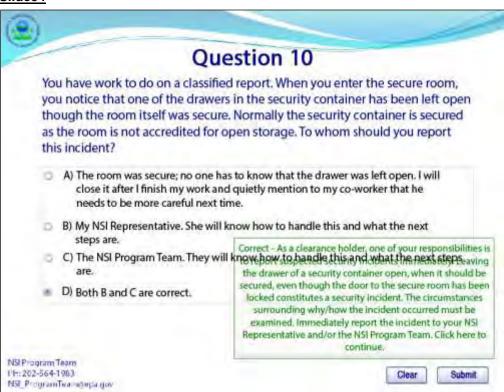


, 26 of 27

Slide53



Slide54



, 27 of 27

The information below supplements the 2013 National Security Information annual training in compliance with requirements specified in 32 CFR 2001 *Classified National Security Information*.

Handling Other Agencies' Materials or Foreign Government Information

At a minimum, all safeguarding and protection requirements identified for the handling of EPA classified information must also be met for classified information generated by and provided to the EPA on behalf of other agencies. Dissemination of other agency materials is allowed if authorized by the owning agency but may be restricted or prohibited. Handling limiters may be included with the information or provided by the owning agency at the time of transfer. In all cases, refer to the owning agency's point of contact for clarification.

In addition to the above guidelines, the following must be applied to foreign government information (FGI):

- Store separately from NSI to ensure on-going protection of the information. This separation may be accomplished by use of separate drawers in a multi-drawer/multi-lock safe.
- Top Secret and Secret FGI must be recorded on a drawer inventory log with a receipt of transmission and/or destruction kept as part of the record, in addition to specific handling requirements identified by the country of origin.
- Reproduction and release of FGI is strictly prohibited, unless expressly granted by the country of origin.
- The recipient of FGI is responsible for ensuring an equivalent degree of protection as required by the country of origin.
- If safeguarding requirements are lower than those required for equivalent US confidential information, then the FGI will be re-marked in the following manner: **This document contains** (insert name of country) information to be treated as US (insert classification level).

Threats and Techniques Employed to Obtain NSI and Penalties for Engaging in Espionage

Foreign intelligence agencies and their agents are motivated to collect classified information in any way possible. These techniques may include:

- Spying on and blackmailing suspected/known clearance holders or other persons of interest
- Surreptitious monitoring of computer access and electronic data collection
- Exploitation of personal relationships

Aiding unauthorized persons in the collection of classified information is considered espionage. Spies may be charged with espionage, theft, computer fraud, and aiding the enemy among other charges. Each charge carries its own minimum term and fines, any combination of which may be applied to the convicted individual. If you suspect you are under surveillance or have been approached by a suspicious individual, report the contact to the NSI Program Team immediately.