



INDUSTRIAL SECURITY

LETTER

Industrial Security Letters (ISLs) are issued periodically to inform cleared contractors, user agencies and DoD activities of developments relating to industrial security. The contents of these letters are for information and clarification of existing policy and requirements. Suggestions for Industrial Security Letters are appreciated and should be submitted to the local Defense Security Service (DSS) cognizant industrial security office. Articles and ideas contributed will become the property of DSS. Inquiries concerning specific information in Industrial Security Letters should be addressed to the cognizant DSS industrial security office.

ISL 2012-04

August 07, 2012

This ISL rescinds Article 16 of ISL 2006-02 and ISL 2011-01 in its entirety, and provides updated guidance regarding the application of Chapter 5, National Industrial Security Program Operating Manual (NISPOM). This ISL further describes the authorized methods for the storage of SECRET and CONFIDENTIAL material. The method of storage selected will be based on the type and size of material to be stored and the ability to meet the specific criteria for each storage option.

1. (5-301) General Services Administration (GSA) Storage Equipment.

GSA-approved storage equipment, within the GSA Federal Supply Schedule, includes modular vaults, which can be used for the storage of classified information. The federal specifications and general requirements are set forth in FED-STD 832, "Construction Methods and Materials for Vaults," dated September 1, 2002. These specifications are equivalent to the criteria found in NISPOM paragraph 5-802, "Construction Required for Vaults."

For additional information, see: <http://www.gsa.gov/portal/content/103856>.

2. (5-303) SECRET Storage.

NISPOM paragraph 5-303 requires SECRET material to be stored in GSA-approved security containers, an approved vault, or closed area, and further prohibits storage using non-GSA approved security containers beginning on October 1, 2012. The Defense Security Service (DSS) places special emphasis on this requirement during recurring assessments. DSS will continue to review contractor plans to meet the deadline, which should include a timetable for identifying and eliminating all remaining non-GSA-approved containers being used to store classified material, and other actions being taken to prepare for this transition (e.g. transfer of classified holdings to other approved storage methods, disposing of classified information, or digitizing essential material). There is no requirement to retrofit locks on existing GSA-approved security containers if the integrity of the container is intact and the GSA label is still

affixed. When locks are determined to be unserviceable, the replacement lock must comply with Federal Specification FF-L-2740.

Additional information can be found on the DoD Lock Program website:

https://portal.navfac.navy.mil/portal/page/portal/navfac/navfac_ww_pp/navfac_nfesc_pp/locks

3. (5-306b) Open Shelf or Bin Storage.

NISPOM paragraph 5-306b states that open shelf or bin storage (hereinafter referred to as “open storage”) of SECRET and CONFIDENTIAL documents in closed areas requires Cognizant Security Agency approval. DSS will consider approving open storage of SECRET and CONFIDENTIAL material and information system (IS) media* in closed areas when the following additional conditions are met:

- The area is limited in size to that required to accommodate storage needs for classified material; or, the operational needs of the work performed in the area warrant open storage.
- The contractor ensures that visitors to such areas without the requisite personnel security clearance and need-to-know for all information stored in the area are denied access to the classified material contained therein.
- Entrance doors to the open storage area are secured by built-in GSA-approved electro-mechanical combination locks that meet Federal Specification FF-L-2740.
- For SECRET material, the area is protected by an approved intrusion detection system with a 30-minute response time, as well as security-in-depth (SID) as determined by DSS. For open storage areas lacking sufficient SID, a 5-minute response time is required.
- For CONFIDENTIAL material, no supplemental protection or SID is required.
- The open storage area is within a facility, or specific portion of a facility, determined by DSS to have security-in-depth based on the following criteria:
 - The contractor has documented the specific layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility, or specified portion of the facility in which open storage is approved. During self-inspections, the contractor must review the effectiveness of these controls and report any changes affecting those controls to DSS.
 - At a minimum, the contractor has considered the following elements in their security-in-depth assessment:
 - Perimeter controls

(*Note: The presence of fixed media such as internal, non-removable hard drives in operational information systems is not considered open storage.)

- Badge systems when the size of the population of the facility render personal recognition impracticable
- Controlled access to sections of the facility in which classified work is performed
- Access control devices when circumstances warrant

While existing DSS-approved open storage areas do not require re-approval, contractors must request DSS approval for open storage if they want to use existing closed areas for this purpose. DSS will evaluate the closed area against the criteria provided above for approval.