



Document Security

June 1, 2015

Fiscal Year 2015 Report to Congress



Homeland
Security

Office of the Chief Security Officer

Message from the Under Secretary for Management

JUN 1 2015

The following report, "Document Security," has been prepared by the Office of the Chief Security Officer.

This document has been compiled pursuant to a requirement in House Report 113-481 accompanying the *Department of Homeland Security Appropriations Bill, 2015*.

Pursuant to congressional requirements, this report is being provided to the following Members of Congress:



The Honorable John R. Carter
Chairman, House Appropriations Subcommittee on
Homeland Security

The Honorable Lucille Roybal-Allard
Ranking Member, House Appropriations Subcommittee on Homeland Security

The Honorable John Hoeven
Chairman, Senate Appropriations Subcommittee on Homeland Security

The Honorable Jeanne Shaheen
Ranking Member, Senate Appropriations Subcommittee on Homeland Security

If you have any questions, please do not hesitate to contact me at (202) 447-3400, or the Department's Chief Financial Officer, Chip Fulghum, at (202) 447-5751.

Sincerely,

A handwritten signature in black ink that reads "RC Deyo". The signature is written in a cursive, flowing style.

Russell C. Deyo
Under Secretary for Management



Document Security

Table of Contents

I.	Legislative Language	1
II.	Background	2
III.	Response	3
	Hard-Copy Document Security.....	3

I. Legislative Language

House Report 113-481 accompanying the *Department of Homeland Security (DHS) Appropriations Bill, 2015*, includes the following requirement:

Document Security

The Committee remains concerned over the need to protect classified information, especially as to methods used to secure paper forms, which can be scanned, faxed, copied, or otherwise stolen or compromised. Existing, off-the-shelf commercial technologies can be used to monitor document access and alert security personnel when sensitive documents are at-risk. The Committee directs the Department to report to the relevant committees of jurisdiction, within 90 days after the date of enactment of this Act, on the measures currently being used to ensure hard copy document security.

II. Background

Current federal standards for the protection of hard-copy, classified materials are described as required under H.R. 113-48. These procedures are longstanding, and the workforce is trained and experienced in these protocols.

III. Response

Hard-Copy Document Security

The Department protects hard-copy, classified documents through a number of means; however, the baseline protections common to all Executive Branch departments and agencies are promulgated through Executive Order 13526, “Classified National Security Information,” and 32 CFR 2001, “Classified National Security Information.” These overarching policies establish requirements for storage in either secure rooms or in General Services Administration (GSA)-approved safes using approved locks; marking documents to indicate sensitivity; handling and access only by those with security clearances; prescribed methods of transportation to and from different locations; and mandatory training for those who might come into contact with such materials. These policies further require that each department and agency appoint a Senior Agency Official (SAO) to provide oversight.

At DHS, the SAO is the Chief Security Officer (6 CFR 7). The Chief Security Officer issued DHS Instruction 121-01-011, “Administrative Security Program,” which is applicable across the Department and implements Executive Order 13526, Classified National Security Information, and 32 CFR 2001, Classified National Security Information. All classified hard-copy documents, at a minimum, are afforded the following protections per this instruction:

1. **Access:** Only those with the appropriate security clearance and need to know may have access to classified information in any form (chapter 3, section 1.A).
2. **Storage:** When not under the control of an authorized holder, documents will be stored in a GSA-approved safe with an approved lock, or in an open storage room meeting specific secure construction standards. Depending on the level of material stored, the room may require additional levels of security such as guards and/or monitored alarms (chapter 4, sections 1-5).
3. **Transportation:** Classified documents must be double-wrapped in opaque, tamper-evident wrapping for transport outside of a building or campus. If hand-carried, the person carrying it must be an authorized courier. For mail, only GSA-approved parcel delivery services or the U.S. Post Office may be used. The type and speed of the service used by a commercial carrier depend on the classification of the document. Generally, hard-copy transport is strongly discouraged in favor of sending it over secure information technology systems (chapter 4, section 7).
4. **Reproduction:** Classified documents may be copied only on approved machines (chapter 4, section 8).

5. **Destruction:** Classified documents must be destroyed by approved methods that prevent reconstruction (chapter 4, section 9).
6. **Marking:** Classified documents must, at a minimum, be marked at the top and bottom of the page with the classification marking, to alert the holder of the sensitivity. Documents that are not working papers must additionally be portion-marked (chapter 9, section 1). Additionally, Standard Form cover sheets are used to both protect the document from casual viewing and to remind the holder of the sensitivity (chapter 14, section 3).
7. **Training:** The Department has an extensive security education and training program. Basic training on the handling of classified materials is required for all clearance holders upon being granted a clearance and every year thereafter (chapter 10, section 1). Furthermore, the Office of the Chief Security Officer offers a variety of other training programs that incorporate the principles of protecting classified information into the curriculum.