Managing Electronic Classified Information Short

Student Guide

September 2016

Center for Development of Security Excellence

Managing Electronic Classified Information Short

Introduction

Technology has become a routine part of our lives. Every day we work and play with various forms of technology at our side—our cell phones, our tablets, our computers. Technology has become so commonplace that we tend to take it for granted. But we cannot become complacent in safeguarding the information that protects our country. Just as we protect our paper-based classified information, we must also protect our electronic forms of classified information that we create, share, and store on computers and other electronic media.

We must be vigilant in protecting our electronic classified information against outside adversaries who are trying to access our classified information through the Internet and against the insider threats who are trying to access our classified information from within.

The National Industrial Security Program Operating Manual (NISPOM) defines a document as “any recorded information, regardless of the nature of the medium or the method or circumstances of recording.” The NISPOM requires you to use the same processes to protect electronic classified documents that you use to protect paper-based classified documents.

These processes are proper marking, retrievability, Top Secret accountability, retention, and destruction. In this Managing Electronic Classified Information Short we’ll examine each of these processes.

The objective for this Short is:

- Identify how to properly manage classified information in an electronic format through proper marking, retrievability, accountability, retention, and destruction

Marking

As stated in the NISPOM (Section 4-200), the purpose of proper marking of classified information is to alert the holder to the degree of protection the information requires. Marking also facilitates downgrading and declassification, and aids in the derivative classification process.

All forms of classified information must be properly marked regardless of the method of safeguarding. For example, even if Secret or Confidential information is stored on a Top Secret (TS) system, the Secret and Confidential information must still be marked with its appropriate classification level.

Do not use information as source of derivative classification if it is not marked in accordance with the NISPOM, is dynamic in nature, such as Wikis and blogs, or if its classification cannot be traced to the original classification authority (OCA).

For more information about properly marking electronic classified information, such as emails, URLs, Web pages, dynamic documents, and blogs, refer to CDSE's Marking in the Electronic Environment Short.

Electronic Media

Here are some guidelines for when to mark electronic media such as DVDs, hard drives and thumb drives.

If the required marking information is stored in readily accessible format on the device, then only the highest level of classified information contained on the device must be marked on the outside of the device. For example, if Confidential and Secret files or documents prepared on an IT system are stored on a compact disc and each file bears its own declassification instructions, the disc does not need to be marked with declassification instructions but does need to be marked with the Secret marking. If the required marking information is not stored in readily accessible format on the device, then all required marking information shall be marked on the outside of the device, normally with a sticker or tag, or placed on documents kept with the device.

Retrievability

According to the NISPOM (Section 5-200), contractors are required to establish an information management system (IMS) to protect and control classified information. The IMS must ensure timely information retrieval from GSA approved containers, data warehouses, and database management systems and disposition of classified information. Contractors must also consider need-to-know for electronic classified information just as need-to-know is considered for paper-based classified information. Partitioning of data is used to segregate information on electronic media to prevent access by those who do not have need-to-know.

Top Secret Accountability

Per the NISPOM (Section 5-201), contractors must establish and maintain access and accountability records for Top Secret material regardless of media type to track duplication and distribution of information and ensure information is available in case of loss or compromise. When reporting loss of Top Secret material on electronic media, identify each individual document on the media. The process for electronic files and media should mirror the process used for printed material and hardware as closely as possible. Each Top Secret document stored on electronic media must be accounted for individually. Review each file, group of files, or data sets individually to determine the best method to account for Top Secret material. For single or multiple related non-human readable files, mark the primary file where possible, or create a label, tag, or accompanying document with appropriate accountability information. In some cases, information may be required to be attached to the CD, hard drive or other media when it is not practical or possible to annotate the files directly. For a hard drive with related files that cannot be individually accounted for or where they are part of a single package, mark the file structure, the individual files or the drive for accountability.

Retention

Per the NISPOM (Section 5-700), contractors are authorized to retain paper-based or electronic classified material received or generated under a contract for two years after a contract is completed, unless the Government Contracting Activity (GCA) approves otherwise. For classified material retained beyond two years, contractors must identify classified material with a list of specific documents for Top Secret information. For Secret and Confidential information, identify classified material by subject matter and approximate number of documents. They must also provide a statement of justification for the retention and obtain the approval of the GCA. Contractors must ensure that a process is in place to ensure that classified electronic files are only retained for the period authorized just as for paper-based classified information.

Destruction

As you know there are various types of IT equipment and electronic media that may store classified information such as magnetic tapes, hard drives, floppy disks, CDs, DVDs, and flash drives. And there are various ways to destroy the classified information contained on electronic media.

Overwriting destroys data by entering new data in its place on solid state storage devices, such as smart cards and flash drives. This method does not declassify electronic media. Therefore the electronic media may only be reused within the same environment.

Degaussing erases data completely from magnetic media such as magnetic tapes, hard drives, and floppy drives.

Sanding and grinding are used to destroy optical media such as CDs and DVDs.

Physical destruction or mutilation is used to destroy destroys all types of paper-based and electronic media by shredding, crushing, disintegrating, pulverizing, and incinerating

Degaussing, sanding, grinding and mutilation all destroy electronic media to the point that it cannot be reused.

For more information on the disposal of classified information, refer to CDSE’s Disposal and Destruction of Classified Information Short.

Review Activity

For each question, select the best response. Check your answers in the Answer Key at the end of this Student Guide.

Question 1. When the required marking information is stored in readily accessible format on electronic media, which of the following must be marked on the outside of the device?

○ All required classification markings, including declassification instructions

○ Only the highest classification level of information contained on the device

○ None; no markings are required on the outside of the device

Question 2. Which of the following methods of destruction allows electronic media to be reused within the same environment?

○ Degaussing

○ Sanding

○ Overwriting

Question 3. What is the standard length of time the NISPOM authorizes contractors to retain paper-based and electronic classified material received or generated under a contract after the contract is completed?

○ 1 year

○ 2 years

○ 5 years

Summary

You must manage, handle and protect electronic classified information the same way you do for paper-based classified information through proper marking, retrievability, Top Secret accountability, retention, and destruction.

You may access additional training, job aids, and resources on managing electronic classified information at www.cdse.edu or www.dss.mil.

Appendix A: Answer Key

Question 1. When the required marking information is stored in readily accessible format on electronic media, which of the following must be marked on the outside of the device?

- ⦿ All required classification markings, including declassification instructions ***(correct answer)***
- ○ Mark the outside of the device.
- ○ Put markings on a document kept with the device.

Feedback: *When information stored on electronic media is in readily accessible format on that media, you must mark the outside of the device with the highest classification level of the information contained on the device.*

Question 2. Which of the following methods of destruction allows electronic media to be reused within the same environment?

- ○ Degaussing
- ○ Sanding
- ⦿ Overwriting ***(correct answer)***

Feedback: *Overwriting destroys data by entering new data in its place on solid state storage devices, such as smart cards and flash drives, so the media may be reused. Because overwriting does not declassify the media, the media must be reused only within the same environment.*

Question 3. What is the standard length of time the NISPOM authorizes contractors to retain paper-based and electronic classified material received or generated under a contract after the contract is completed?

- ○ 1 year
- ⦿ 2 years ***(correct answer)***
- ○ 5 years

Feedback*: The NISPOM authorizes contractors to retain paper-based and electronic classified material received or generated under a contract for two years after the contract is completed, unless the Government Contracting Activity requires otherwise.*