Storing Government Classified Data

Requirments for such storage by Contactors

By Charles Widger, 11/19/2025, Ver 4

Introduction

Donald Trump Indicted for Retention and Improper Storage of Materials

- On 8 August 2022 the FBI executed a search warrant of the residence of Donald Trump at Mar-a-Lago.
  - Over 13,000 government documents were obtained from Trump from this search and others.
    - Of these, 337 were classified. The August search yielded 102 of these. Two more were later found at other locations.
    - 48 empty folders with classification markings were also found.
- On 8 June 2023, Trump was indicted on charges related to these documents.
  - On 13 June, he surrendered to Federal custody, was arrested, booked, processed, and arraigned in U.S. District Court in South Florida.

Photo by US Dept of Justice
Only cover pages are shown. These apply to both front and back and show no classified information, only highest level and access restrictions.

Development of Control

A Short History of Securing Government Information in the USA

- March 22, 1940
  - Franklin Roosevelt signs Executive Order 8381, which creates 3 levels of security: Restricted, Confidential, Secret.
- February 1, 1950
  - Harry Truman signs Executive Order 10104, which creates security level Top Secret.
- November 5, 1953
  - Dwight Eisenhower signs Executive Order 10501. This removes level “Restricted.” It removes classification authority from 28 government entities and limits its use in 17 others. It provides classification guidelines for the three remaining levels, Confidential, Secret, Top Secret.
  - The Pentagon creates labels for “Special Access” to isolate classified information from outside intended use.
- March 8, 1972
  - Richard Nixon signs Executive Order 11652 to legitimize the use of Special Access controls and use of “Special Access Program.”
- January 6. 1993
  - George H. W. Bush signs Executive Order 12829. It creates the National Industry Security Plan (NISP) and corresponding operation manual, (NISPOM). It makes changes to assist the sharing of information between security entities.

National Industry Security Plan

NISP and Associated NISPOM

- Before 1993, the Department of Defense issued its own plan and operating manual for how contractors were supposed to handle classified information, DoD 5220.22 and DoD 5220.22-M. This is the basis for the current NISP and NISPOM.
  - Other agencies had their own plans and operating manuals.
- The current NISP was established in 1993 by Executive Order 12829.
  - The NISP recognizes 4 agencies: the Department of Defense, the Department of Energy, the Central Intelligence Agency, and the Nuclear Regulatory Commission.
    - These have subagencies. A total of 35 agencies are affected.
  - The NISP and NISPOM have undergone several revisions, especially as it has been effected by changes in technology, especially computing.
- All the classified materials from Trump were created by processes consistent with the NISPOM.

Public Perception of Security

As reflected by the NBC Program *Blindspot* (2015-2020)

- Program Premise
  - A large bag is left in New York City at Times Square. Those leaving it are not identified and they disappear. A bomb squad is called in to see if it is safe. The bag is unzipped, and out steps a pretty, very fit, young woman covered only by tattoos (and a pair of 3 inch heeled shoes). A large display on her back, shoulder to shoulder, names FBI Agent Kurt Weller, who gets assigned to the case of determining who this woman is, and whether there are any associated threats.
  - The woman speaks fluent English (and several other languages), but has no recollection of who she is, her name, where she came from, or what she is to do. She is given the name Jane Doe, clothes to wear, a place to stay and groom, and food to eat.
  - It later develops she is the daughter of a female ex-US army general who is planning to ursurp the US Government. She has a brother, with whom she grows up. The two are expert in various kinds of Gung Fu, even better than their master teachers. The tattoos give hints as to the crimes the mother commits, which are well-hidden, and eventually solved by Kurt Weller and his team of various experts with the help of Jane and her tattoos.
- Some factual errors about security in the program:
  - There is are an ascending level clearances to go beyond the actual three: confidential, secret, top secret.
  - The Vigenère encryption, founded in 1553 is completely secure - it was broken in 1863. I spoke to this in my presentation on Information Theory.

Other Kinds of Data Classification

Looking past Government Classification

- Datamation, an on-line magazine dealing with computing, established in 1957.
- Microsoft, a noted local supplier of computing and related products.
- NIST, National Institute of Standards and Technology, an agency under the Department of Commerce. This function is required by the Constitution under Article 1, Section 8.
- University of Missouri, a noted university founded in 1839 and located in Columbus, Missouri.

Some Basic Principles

From the NISP and NISPOM

- There are 3 levels of classification, Confidential, Seceret and Top Secret. Something not classified has no classification level. Being granted access to these levels is determined by some kind of investigation to determine whether the person and employer can be trusted. There are briefings to teach the affected of their responsibilities.
- There are restrictions on the places where these materials can be held and discussed, to limit the risk due to bugging. Where personal cell phones may be taken are also limited because they may be turned into listening devices, even without the owner's knowledge.
- There can also be restrictions on who has access to materials. One basic condition is need to know, such as being work related to some contract that requires it. Other kinds of restrictions apply to Sensitive Compartmented Information (SCI). Further, there are Special Access Program qualifications, such as COMSEC (Communications Security).
    - Note that a cover page in the Trump materials included SCI. This puts additional restrictions on the places where such materials can be stored and used. An inspected, monitored, and approved place for SCI is a SCIF (SCI Facility). For a trial for Donald Trump, this would have to include the court facilities.
- Entities must be given written information about the kind of information they are to control. They then produce and maintain a classification guide. These can change of time. Since handling classified data is labor intensive, these agencies are encouraged to de-classify as risk decreases. Common knowledge, such as 2 + 5 = 7, is never to be classified.
- People approved for any level and information are periodically briefed and re-investigated.

NISP

National Industry Security Plan

- Control of Classified Information changed following the 9/11/2001 attacks.
  - The Office of the Director of National Intelligence (ODNI) was created as a Cabinet position. The Senate approves nominees.
  - Processes are now more uniform across the affected offices
- Source: National Archives
  - Full text
  - Size: 27 pages as PDF
- Introduces Sensitive Compartmented Information (SCI)
  - SCI may involve information at any classification level.
  - Controls who may have access and the circumstances of how it is stored and used.
- Introduces Special Access Program
  - Example: COMSEC

NISPOM

What to do and how to do it

- Source: National Archives
  - Full Text
- Size: 122 pages as PDF
- Particular items of interest regarding Trump materials:
  § 117.9 Entity eligibility determination for access to classified information.
  § 117.10 Determination of eligibility for access to classified information for contractor employees.
  § 117.12 Security training and briefings.
  § 117.13 Classification.
  § 117.15 Safeguarding classified information.

On Learning More

- There are several models for implementation of secure systems.
  - Bell-LaPadula
  - Biba Integrity Model
  - Clark-Wilson
  - Multilevel Security (MLS)
  - The Common Criteria for Information Technology Security Evaluation