



## **ISOO Notice 2023-001: Classified Records Found Outside Government Control**

---

June 21, 2023

### **Authorities**

1. Executive Order 13526, “Classified National Security Information”
2. 32 CFR 2001.36, “Classified Information in the custody of private organizations or individuals”

### **Purpose and Background**

The purpose of this ISOO Notice is to provide guidance to organizations and individuals outside of government control who come across potentially classified records in their holdings or possession on identifying, protecting, and transmitting classified records.

Former government officials, employees, and contractors have been known to retain papers related to their time in public service that may inadvertently contain classified national security information.

Often, it is not until these records are donated to private archives or other institutions and formally processed that archivists and others processing these papers realize a collection contains classified information. If an archive or a library has not received federal approval to store classified materials, continuing to store the records in an unapproved area could be endangering national security. In these instances, the institution should contact the Information Security Oversight Office (ISOO) at the National Archives and Records Administration and arrange for these records to be securely stored. ISOO will maintain temporary custody of the records through the declassification process.

By contacting ISOO, institutions and individuals will be respecting the access restrictions placed on that information by the U.S. government. ISOO, in turn, will respect the rights of the institution to maintain the integrity of collections of donated personal papers.

The regulatory authority regarding this program is as follows:

32 CFR 2001.36(b): “Anyone who becomes aware of organizations or individuals who possess potentially classified national security information outside of government control must contact the Director of ISOO for guidance and assistance. The Director of ISOO, in consultation with other agencies, as appropriate, will ensure that the safeguarding and declassification requirements of the Order are met.”

## Guidance for Identifying Classified Records

There are three basic criteria that can be applied to determine whether a document contains classified information:

- The information should concern the national security of the U.S. government. If the document was created by a private organization or a state government agency, it may contain classified national security information only if the organization or agency was authorized to do so by the U.S. government. Certain defense contractors and research laboratories are examples. Also, the information should not concern personal, private, or purely political issues. Over the decades, many documents have been stamped “Confidential” not because they would damage national security if released, but to indicate some other type of sensitivity. When in doubt, consider the document classified and contact ISOO for assistance.
- There should be a classification marking (i.e., Top Secret, Secret, or Confidential) on the top and bottom of every page of the document. Older documents may have markings only on the top of the first page. In more recent documents, individual paragraphs may also be portion marked with markings like “(S)” for Secret or “(C)” for Confidential.
- The document should not be marked as declassified. A declassification marking should look like an official stamp that indicates the name and office of the person who authorized the declassification action. A copy of a declassified document from the National Archives and Records Administration should include a marking that includes a project number starting with “NND” or “NW.”

While these are the primary means of identifying classified information, those who suspect they have classified materials in their collections should also be careful to examine documents for:

- **“Restricted Data” and “Formerly Restricted Data” markings.** These designations refer to categories of classified information concerning nuclear weapons design and utilization. Despite the misleading nature of the phrase “Formerly Restricted Data,” documents with this marking remain sensitive and must be protected.
- **Unmarked Classified National Security Information.** Records of national security officials should be reviewed and handled carefully, as the classification marking requirements may not always have been executed on informal records such as handwritten notes. In all cases, it is the sensitivity of the information that determines classification. An unmarked, handwritten page can just as easily contain classified national security information as a document containing classification markings. When in doubt, treat handwritten notes concerning intelligence, military, diplomatic, or emergency planning matters as classified national security information.
- **Declassification Dates.** Some documents may have been originally marked with a date on which the document may be declassified. These dates are useful in determining the relative sensitivity of the information contained in the document, but occasionally these

markings are erroneous or invalid. Remember that regardless of markings, only a U.S. government declassification authority can declassify classified information.

- **Foreign Government Information.** Foreign governments routinely share classified information with the U.S. government. Foreign government information received by a U.S. government agency with a promise of non-disclosure should remain protected, but in some cases, information may be declassified and released. Many foreign markings resemble U.S. markings.
- **Controlled Unclassified Information.** Federal agencies have designated some types of information as requiring a degree of control that but that is not classified national security information. These types of markings may include “Controlled Unclassified Information,” “CUI,” “For Official Use Only,” “Limited Official Use,” or “Sensitive but Unclassified.” These types of markings do not designate classified national security information. Archivists processing papers containing U.S. government information should not release social security numbers for living people, health care information, and other personal information collected from private citizens.
- **Closed Congressional Information.** Archivists processing the papers of former congressmen should be aware that the rules of the U.S. Senate and the House of Representatives restrict public access to certain types of closed committee and investigative records, regardless of whether they contain classified national security information, for up to 50 years.
- **Codeword Information.** Since World War II, when the British used the word “Ultra” to designate intelligence obtained by cracking the German Enigma encryption machine, the most sensitive types of U.S. government information have been identified by special codewords. These include intercepts of encoded enemy radio signals, information about satellite reconnaissance programs, and human intelligence programs. Words like “Umbra,” “Talent-Keyhole,” “Ruff,” or “Gamma” on records also carrying a “Secret” or “Top Secret” classification marking, indicate something particularly damaging to national security if improperly released, regardless of the age of the records.

### **Guidance on Storing and Protecting Classified Records**

If institutions or individuals discover classified materials in their holdings and they do not have federally approved secure storage, they should immediately remove the records from public review and restrict access to as few individuals or staff members as possible. Until they are ready for transmittal to ISOO, the records should be locked in a safe, filing cabinet, or other secure areas.

### **Guidance on Transmitting Classified Records**

Transmittal requirements for classified materials vary depending on the classification level of the information they contain. In all instances, the use of street side mailboxes is prohibited.

CONFIDENTIAL materials may be sent via U.S. Postal Service certified, first class, express, or registered mail or government courier service.

SECRET materials may ONLY be sent via U.S. Postal Service express or registered mail or government courier service.

When mailing materials to ISOO, please adhere to the following guidelines:

Wrap the body of records in opaque paper. Heavy brown paper or brown mailing envelopes are best. CONFIDENTIAL and SECRET materials may be wrapped together.

Seal all seams with filament tape.

Address the package to:

**Director, Information Security Oversight Office  
National Archives and Records Administration  
700 Pennsylvania Avenue NW, Room 503  
Washington, DC 20408**

Provide a return address.

Label the front and back of the package with the highest classification marking of the documents it contains.

Wrap the entire package ONCE MORE in opaque paper.

Again, address the package to the Director of ISOO as indicated above and provide a return address.

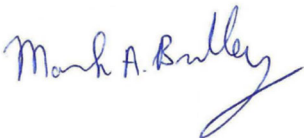
On this outer wrapper, do NOT write the classification level of the materials contained within.

Again, seal all seams with filament tape.

TOP SECRET materials may NOT be sent via U.S. mail and may only be transmitted by authorized government courier service. ISOO can make the necessary arrangements on the institution's behalf.

ISOO staff will give more detailed instructions regarding the shipment of classified records and the temporary retention of records by ISOO pending declassification.

Please direct any questions regarding this ISOO Notice to: [isoo@nara.gov](mailto:isoo@nara.gov).

A handwritten signature in blue ink that reads "Mark A. Bradley". The signature is written in a cursive style with a long, sweeping tail on the letter "y".

MARK A. BRADLEY  
Director