



Restricted Data (RD) & Formerly Restricted Data (FRD)

Since their introduction at the end of World War II, nuclear weapons have been seen as so radically different from other weaponry, so uniquely destructive, that extraordinary measures are needed to slow their spread. To this end, the Congress enacted the Atomic Energy Act to assure firm government control over all aspects of nuclear technology relating to the creation, design, production or use of nuclear weapons. Information that is designated "Restricted Data" and "Formerly Restricted Data" is classified under the authority of the Atomic Energy Act of 1954 and is under the jurisdiction and control of the Department of Energy (DOE).

General:

The Atomic Energy Act is the basis for classification of atomic energy information. In accordance with the Atomic Energy Act, all atomic energy information is classified unless a positive action is taken to declassify it. This is directly opposite to procedures used for information classified by E.O. 13292. This is a significant difference that should be clearly understood. By the Act, Congress has decreed that atomic energy information is different – it is "born classified," it may be declassified only by the Department of Energy. No other organization can declassify atomic energy information.

"The term Restricted Data means all data concerning,

- (1) design, manufacture or utilization of atomic weapons;**
- (2) the production of special nuclear material; or**
- (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to Section 142."**

"Formerly Restricted Data" (FRD) is information which has been removed from the Restricted Data category after the DOE and the DoD have jointly determined that the information relates primarily to the military utilization of atomic weapons and can be adequately safeguarded as National Security Information in the U.S. Such data may not be given to any other nation except under specially approved agreements and with the authorization of DOE. FRD is identified and handled as Restricted Data when sent outside the U.S.

Declassification:

Documents marked as containing RD and FRD remain classified until a positive action by an authorized person is taken to declassify them; no date or event for automatic declassification ever applies to RD and FRD documents. Only the DOE may declassify contractor documents marked as



Restricted Data (RD) & Formerly Restricted Data (FRD)

RD. Contractors shall send any document marked as RD or FRD that must be declassified or sanitized to the appropriate government contracting office.

Marking:

In addition to the markings specified in Chapter 4 of the National Industrial Security Program Operating Manual (NISPOM), classified material containing RD and FRD shall be marked as indicated below:

*Restricted Data: The following notice shall be affixed on material that contains Restricted Data. This may be abbreviated RD.

Restricted Data:

This material contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to administrative and criminal sanctions.

Material classified as RD must indicate the classification guide and the authorized RD classifier. The following marking shall be applied:

Classified by: (guide)

Classifier: (name and title)

*Formerly Restricted Data: The following notice shall be affixed on material which contains Formerly Restricted Data. This may be abbreviated FRD.

Formerly Restricted Data:

Unauthorized disclosure subject to administrative and criminal sanctions. Handle as Restricted Data in foreign dissemination. Section 144b, AEA 1954.

Material classified as FRD must indicate the classification guide. The following marking shall be applied:

Classified by: (guide)

Personnel Clearances (PCL):

Personnel with a final Secret PCL or final Top Secret PCL may have access to RD and FRD at their level of clearance and lower levels. Personnel with an interim PCL may only have access to FRD at the level of their interim clearance and lower levels.

Reporting:

The loss, compromise or suspected compromise, or an indication that RD or FRD information may have been made available to unauthorized persons (even if they have the proper clearances) must be immediately reported to the local Facility Security Officer or designated alternate.



Restricted Data (RD) & Formerly Restricted Data (FRD)

ACKNOWLEDGMENT: I have been briefed on RD/FRD by SAIC and will comply with all protection requirements.

PRINTED NAME

EMPLOYEE NUMBER

SIGNATURE

DATE (MM/DD/YYYY)