UNITED STATES DEPARTMENT OF AGRICULTURE
FOOD SAFETY AND INSPECTION SERVICE
WASHINGTON, DC

# FSIS DIRECTIVE	1300.2	1/25/88

CONTRACTOR ACCESS TO FSIS DATA BASES

I. PURPOSE

To establish policy on contractor access to FSIS data bases.

II. (RESERVED)

III. REASON FOR ISSUANCE

A. Assigns responsibility and provides detailed procedures for the control of automated data processing contractor access to FSIS data bases.

B. Provides for systems security in an adequate and consistent manner.

IV. REFERENCES

FSIS Directive 1300.1, FSIS Information Resources Management.

V. FORMS AND ABBREVIATIONS

The following will appear in their shortened form in this directive:

ASD	Administrative Services Division
COTR	Contracting Officer's Technical Representative
FOIA	Freedom of Information Act
IEDM	Industrial Engineering and Data Management Division
PD	Personnel Division
OPI	Office of Primary Interest

VI. DEFINITIONS

A. **Read/Print Only Access.** User may read, extract and perform various calculations using data in the system. User cannot add, edit or delete records, or in any way change the information/program residing in the data base.

B. **Execute Access.** User has full unencumbered access to data base. User can alter data base and information contained therein.

C. **Account.** A code, usually for a group of individuals (such as a division), for controlling access to data, charging for system use, and creating an audit trial of user access.

D. **User Structure.** The combination of access level (s) and data bases available to a user.

E. **Office of Primary Interest.** The program or staff which "owns" the data base to be accessed. The term 'owns" indicates that the program or staff had the data base developed and is generally responsible for its control.

VII. POLICY

To control contractor access to FSIS data bases in a manner that is consistent throughout the Agency and sufficient to protect the data base systems and sensitive information.

VIII. DELEGATIONS OF AUTHORITY

All FSIS data bases are controlled under the authority of the Administrator. Specific authorities are delegated, as follows:

A. FOIA Officer determines data/system sensitivity in relation to the FOIA and the Privacy Act, at the request of programs/staff which have data bases.

B. The Employment and Employee Benefits Branch, PD, determines personnel security clearance requirements regarding data base access, at the request of programs/staff which have data bases.

C. The contracting officer, ASD, obtains security clearances for contractor personnel. The contracting officer also communicates with prospective vendors subsequent to solicitation, and handles any modification, clarification, or complaints pertaining to an awarded contract.

D. COTR interfaces with the contractor, program/staff and contracting officer on all technical matters.

E. The OPI exercises control over its data bases.

F. The manager of the program/staff sponsoring the contract (or the COTR, if one has been designated) determines contractor needs, coordinates data base security and obtains access for the contractor to the necessary data bases.

G. IEDM establishes the user structures for individual contractor employees and controls passwords.

IX. RESPONSIBILITIES

A. The manager of the program/staff sponsoring the contract (or the COTR, if one has been designated):

1. Determines which FSIS systems/data the potential contract needs access to.

2. Determines the data/system sensitivity in coordination with the FOIA Officer.

3. Determines the security clearance requirements, if any, in coordination with the Employment and Employee Benefits Branch, PD.

4. Contacts the OPI (the OPI's for most data bases are listed as contacts in the FSIS ADP Systems Inventory), explains the type of access needed and obtains written approval. The OPI will often be the unit sponsoring the contract. Basic types of access are: Read/print only, execute, or access by running programs/combining with other data.

B. The contracting officer, ASD:

1. Includes security clearance requirements in the procurement document (more than one level of clearance may have to be specified).

2. Arranges with PD for appropriate security clearances for individuals named in the contract bid(s). Contractor work cannot start until the clearances are obtained. Failure to obtain clearances on the contractor's proposed personnel makes the bid/proposal non-responsive.

3. Mails the solicitation to prospective vendors (bidders). Only the contracting officer communicates, verbal or written, with the vendors.

C. The COTR is the vendor's contact person relating to technical matters after the award. The contracting officer handles all administrative matters and any modification, clarification of contract terms, or complaint pertaining to the contract.

D. The program/staff COTR:

1. Obtains an account and user structure with passwords having the specifically approved access capability and no other capability. IEDM sets the structure in place for individual contractor employees, according to security clearances and approved access level.

2. Arranges for IEDM to provide a systems orientation for the contractor.

3. Checks the account and user structure of the contractor's personnel against those which were provided to ensure that they have the specific approved access capability and no other capability.

4. Notifies IEDM when the contract is completed and when contractor personnel change, so that IEDM can withdraw passwords.

Deputy Administrator
Technical Services