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

FSIS DIRECTIVE	1300.15	2/5/08

CONTROLLED ACCESS TO RESTRICTED AREAS

I. PURPOSE

This directive:

A. Establishes policy and provides procedures for Office of the Chief Information Officer (OCIO) employees who have access to the FSIS Network and Server rooms to ensure that an appropriate level of security is maintained.

B. Prescribes OCIO employee’s responsibilities for controlling the use and access of the FSIS Network and Server rooms.

C. Addresses escort requirements for unauthorized personnel accessing the FSIS Server and Network rooms.

II. BACKGROUND

The FSIS Network and Server rooms house Agency computing equipment and hardware supporting the needs of FSIS. Security of the FSIS Network and Server rooms must be managed and controlled by a responsible branch within OCIO. Equipment must be protected from risks that could result from tampering or destruction.

III. (RESERVED)

IV. REFERENCES

DM 3510-001	Physical Security Standards for Information Technology (IT) Restricted Space

DISTRIBUTION:
All Offices (Except Circuit Supervisors and Below)

OPI:
OPEER – Information Technology Policy and Capitol Planning Division

V. ABBREVIATIONS

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

CIO	Chief Information Officer
CNSD	Computer and Networking Support Division
NB	Networking Branch
OCIO	Office of the Chief Information Officer

VI. DEFINITIONS

A. **Computing Equipment**. Servers, routers, switches, hubs, computers, peripheral equipment, etc.

B. **Employee**. An individual currently working for FSIS, whether full-time, part-time, intermittent, or on a contract basis.

C. **Network and Server Rooms**. Designated restricted spaces that house computer and telecommunications equipment and local area networks.

VII. ROLES AND RESPONSIBILITIES

A. **OCIO**. The CIO and Deputy CIO promote and support effective security access standards for the FSIS Network and Server rooms.

B. **CNSD**.

1. The Director ensures that policy is enforced to protect network integrity.

2. The NB Chief collects and maintains the FSIS Network and Server room logs.

3. The senior OCIO staff members at field locations maintain the FSIS Network and Server rooms outside of Washington, D.C.

4. All OCIO personnel with access authority to the FSIS Network and Server rooms must be aware of Agency policy and their obligations. OCIO personnel must ensure their duties are performed in a professional manner while working in any the FSIS Network and Server rooms.

5. The authorized NB staff member escorting visitors is responsible for making visitors aware of this policy. An authorized NB staff member must accompany visitors who access the FSIS Network and Server rooms.

VIII. MONITORING

Access into and out of the FSIS Network and Server rooms is monitored by the CNSD Director and the NB Chief via the access logs. Any discrepancy with work schedules against the access log will be investigated and the appropriate action will be taken.

IX. RESTRICTED ACCESS POLICY

A. The FSIS Network and Server room doors must remain closed and locked at all times.

B. Only individuals with access rights will have authorized access. Access will be granted via electronic badge, cipher lock, or key. When the FSIS Network and Server rooms are secured by a key, no master key will be made. Each FSIS Network and Server room key must be made individually for each door.

C. Physical access to the FSIS Network and Server rooms will be limited to those with a work-related need to enter.

D. The access list for authorized, unescorted persons is maintained by the NB Chief or the field representative responsible for the FSIS Network and Server rooms. The list will be posted in the FSIS Network and Server rooms. (**NOTE**: Exceptions for access will be authorized by the CNSD Director in consultation with the CIO.)

E. Unescorted access to the FSIS Network and Server rooms will be granted to CNSD staff members who require routine physical access to equipment for performing their primary job functions. All other designated individuals on the access list will have unescorted access privileges.

F. Visitors will be accompanied by an authorized escort at all times. Escorts must ensure that visitors follow all appropriate protocols. Access to the FSIS Network and Server rooms can be arranged during normal business hours.

G. Emergency after-hours access will be accommodated. Anyone requiring emergency access must call the FSIS Service Desk at (202) 720-4016 or (800) 473-9135. If no one is available, leave a voice message with a name, contact phone number, and reason for needing access. An NB staff member will return all calls as soon as possible for after-hours emergencies.

H. All requests for unescorted access rights must be made in advance and in writing to the CNSD Director or the responsible field representative.

I. All FSIS Network and Server room tours must be pre-approved by the CIO.

X. PROCEDURES

A. Only FSIS employees with an ongoing recurring business need will be granted unescorted access to the FSIS Network and Server rooms.

B. USDA-issued photo Identification is required for all personnel and must be displayed at all times.

C. Visitors must display a visitor's pass at all times.

D. Visitors to the FSIS Network and Server rooms must sign in and out on the access logs and must be escorted at all times by an authorized escort. (**NOTE**: Cleaning and maintenance personnel will be escorted at all times by an authorized individual.) The access log will be retained by the NB Chief or the responsible field representative.

E. Employees who no longer have a business need to enter the FSIS Network and Server rooms will immediately be removed from the access list.

F. Visitors must be kept to a minimum.

G. All escorted visitors must sign in and out on the access log. The logbook will contain the:

1. Visitor's printed name.

2. Visitor's signature.

3. Visitor's Agency name.

4. Visitor's office name.

5. Visitor's company name.

6. Purpose for the visit.

7. Date and time the visitor signs in and out.

8. Escort's printed name.

9. Escort's signature.

H. An individual with knowledge of the system being accessed will escort non-permanent contractors to the FSIS Network and Server rooms.

I. The CNSD Director will conduct quarterly access reviews of designated personnel with ongoing business in the FSIS Network and Server rooms. (**EXAMPLE**: Maintenance workers.)

J. The use of mobile phones, pagers, laptops, or other equipment that emits radio waves is not permitted within the FSIS Network and Server rooms in areas that process classified information.

K. The NB Chief or the responsible field representative will perform monthly reviews and sign off on the FSIS Network and Server room access logs.

L. The NB Chief or the responsible field representative maintains all original FSIS Network and Server room access logs at their location. The logs and personnel access lists will be maintained in a binder for one year and are available for review.

Assistant Administrator
Office of Management