CHAPTER 5 - PART 1
USDA INTERNET ACCESS SECURITY FOR PRIVATE INTERNET SERVICE PROVIDERS

1 BACKGROUND

USDA DR 3300-1, Telecommunications, Appendix I, authorizes use of the Internet to support Departmental and agencies missions and responsibilities through the access and use of authorized remote information systems. When agency or staff office Internet requirements cannot be met through use of the USDA Internet Access Network, a technical exception must be obtained from the Office of the Chief Information Officer (OCIO), Office of Cyber Security, for access to a private Internet Service Provider. The Office of the Inspector General (OIG) performed an audit of Information Resources Management controls in the use of the Internet and found potential vulnerabilities to the Department and recommended security provisions to protect USDA data. This chapter responds to security issues identified in Audit Report 50099-7-FM, USDA Access to the Internet and Audit Report 23099-1-FM, OCIO Security Over Data Transmission in the Department Needs Improvement.

2 POLICY

a Mandatory Use of USDA Internet Access It is USDA policy that agencies and staff offices will use only the USDA Internet Access Network for entry to the Internet. In the past, agencies were granted exceptions to use private Internet Service Providers (ISP) based on the limited scope of the USDA Internet Access Network. Since that time, the department has greatly expanded the scope of Internet access provisioning and can satisfy most of USDA's current requirements. Therefore, all existing exceptions for the use of private Internet Service Providers are rescinded upon issuance of this policy.

b International Internet Access It is policy that USDA agencies located in overseas facilities should make every reasonable effort to obtain Internet access from

private Internet Service Providers that can meet the security requirements of this policy. Activities that are co-located with State Department Embassies should explore obtaining Internet service using their government-wide contracts or other Federal agencies International Service contracts. In any case, the need for security should be based on the following factors:

- Sensitivity of data transmitted;
- The potential harm that might result from hackers using agency facilities as a back door to gain access to USDA networks.

If the Internet is used to research information required by the agency, every effort should be made to ensure that the device used to access the Internet is a stand-alone machine or using a proxy server, not part of any USDA network.

All ISP exceptions are to be submitted to the Office of Cyber Security through the OCIO, Office of Information Resources Management.

c Policy Exception Requirements – Agencies will submit all policy exception requests directly to the ACIO for Cyber Security. Exceptions to policy will be considered only in terms of implementation timeframes; exceptions will not be granted to the requirement to conform to this policy. Exceptions that are approved will be interim in nature and will require that each agency report this Granted Policy Exception (GPE) as a Plan of Action & Milestone (POA&M) in their FISMA reporting, with a GPE notation, until full compliance is achieved. Interim exceptions expire with each fiscal year. Compliance exceptions that require longer durations will be renewed on an annual basis with a updated timeline for completion. CS will monitor all approved exceptions.

3 RESPONSIBLITIES

a The Associate CIO for Cyber Security will:

(1) Provide customer support to agencies and staff offices regarding exceptions to the use of the USDA Internet Access Network;

(2) Analyze and review exception documentation that includes obtaining technical assurances from the Office of Telecommunications Services (TSO) that this location cannot be feasibly served. Sites using private ISPs that have had previous IT Security Incidents will be subject to especially close scrutiny;

(3) Review security documentation to ensure that agency verification of security controls provided by the private ISP is strong in terms of meeting departmental requirements and Office of Management and Budget circulars and memoranda concerning Privacy Policy and Data Collection.

(4) Review the Agency Annual Cyber Security Plan to ensure that the plan addresses in detail the security provisioned for each site that uses a private Internet Services Provider, including a certification on Privacy Policy.

(5) Maintain a database of approved private ISPs used by the agencies/staff offices in lieu of the USDA Internet Access Network; and annually review the database for possible migration candidates to the USDA Internet Access Network.

b The Associate CIO for the Office of Telecommunications Services will:

Review all ISP exceptions and provide assurances that the USDA Internet Access Network cannot technically provide the capability requested and that the network will not be negatively affected if a private ISP is used.

c The Associate CIO for Information Resources Management (IRM) will:

(1) Support the policy and procedures contained in

this manual to ensure that appropriate security protection is provided to all USDA managed networks, systems and servers; and

(2) Receive, review, and coordinate a response with the Associate CIO for Cyber Security to any exception requests to this policy.

d Agency Chief Information Officer will:

(1) Designate an appropriate Senior Level Manager (who may be the CIO or other designated official) to be the Certifying Official (CO) for all private Internet Service Providers provisioned;

(2) Require the CO to certify on behalf of the agency/staff office compliance with all requirements of this Departmental Manual for use of newly approved private ISPs;

(3) Notify the Office of Cyber Security in writing of all existing uses of private ISPs. The list, signed by the CO within 60 days of this notice, will include the agency name (including subunit name, if appropriate), location, supplier of existing internet access, and an agency Point of Contact (including name and telephone number) at every location.

(4) Review all existing private ISP provisioning within the agency and forward exception requests signed by the CO for those locations that cannot be technically provisioned under the USDA Internet Access Network.

(5) Provide a compelling technical justification for the continued use of a private ISP to include language concerning the provider's ability to provide strong security safeguards and privacy protection measures. All exception packages should include the following security information:

(a) A description of security controls in place protecting USDA information systems and

data against unauthorized intrusion for each site;

(b) Documentation, including the Agency Annual Cyber Security Plan, which defines security features available from each provider as well as a list of security features implemented;

(c) Documentation which specifically details each site's compliance with DR 3140-2; National Institute of Standards and Technology (NIST) Special Publications 800-12, An Introduction to Computer Security, and 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems; and Office of Management and Budget (OMB) Circular A-130, Appendix III.

(6) Modify the provisioning arrangements for any site technically feasible location to the USDA Internet Access Network within 30 days of this policy issuance;

(7) Each agency CO will certify that all newly approved private ISPs comply with OMB Privacy and Data Collection Policies for each entry point. This includes privacy posting that is clearly labeled and easily accessed when someone visits a web site. In addition, private ISPs will not use persistent "cookies" at Federal web sites they maintain unless there is a clear and compelling need as defined in OMB Memo M-00-13 and other OMB and CS guidance on Privacy.

(8) Each agency will use department recommended encryption methods to protect data transferred over any private ISP to and from the USDA Internet Access Network.

-END-