

APPENDIX I

INTERNET

1 PURPOSE

This Appendix establishes policy for the management and use of the Internet in the United States Department of Agriculture (USDA).

2 BACKGROUND

USDA authorizes the use of the Internet to support Department and agency missions. Access to the Internet is provided through the USDA Internet Access Network. Internet is an integral part of service delivery in USDA. While its rate of growth continues to increase, today the Internet, a world-wide "network of networks" comprises roughly 200,000 networks ranging from intra-building local area networks to global wide area networks. High speed networking technologies and developments have made the Internet a desirable source for expanding research interest and information dissemination and communications. More recently the Internet has expanded to include government information, educational information systems, archives and business resources. The Internet also includes functions for electronic mail (E-Mail), remote computer networks, file transfers, World Wide Web (WWW) and wide area information servers. USDA recognizes that the Internet differs from existing earlier communications systems and that policy must reflect that the Internet has no geographical boundaries, USDA employees should understand how the Internet operates, how to use it, and how it affects program delivery today and its promises for tomorrow.

3 REFERENCES

<u>Source</u>	<u>Publication</u>	<u>Title/Subject</u>
GSA Systems	41 CFR Subpart	Use of Government Telephone
101-35.1	Internet Request for Domain Requirements	

Network Comment Information (RFC) 920 Center

(InterNIC)

InterNIC RFC 1087 Ethics and the Internet Federal RFC 2146 U.S.
Government Internet

Networking Domain Names Council

NIST Computer Connecting to the Systems Internet: Security Laboratory
Considerations (CSL) Bulletin July, 1993

NIST FIPS PUB 95-1 Codes for the Identification of
Federal and Federally Assisted Organizations

USDA DR 3140-2 Internet Security

USDA/OCIO/NSD Guide to the USDA Internet

4 ABBREVIATIONS

ARPA - Advanced Research Projects Agency

AS - Autonomous System

ASN - Autonomous System Number

CIO - Chief Information Officer

CO - Certifying Official

CSL - Computer Systems Laboratory

DNS - Domain Name System

EN - Enterprise Network

FPMR - Federal Property Management Regulation

FTS2000 - Federal Telecommunications System 2000

IAB - Internet Activities Board

InterNIC	-	Internet Network Information Center
IP	-	Internet Protocol
ISP	-	Internet Service Provider
ISSPM	-	Information Systems Security Program Manager
ISSTD	-	Information Systems Security and Telecommunications Division
LATA	-	Local Access and Transport Area
NIC	-	Network Information Center
NIST	-	National Institute of Standards and Technology
NSD	-	Network Services Division
OCIO	-	Office of the Chief Information Officer
OMB	-	Office of Management and Budget
POC	-	Point of Contact
RFC	-	Request For Comment
SIRMO	-	Senior Information Resource Management Official
TCP/IP	-	Transmission Control Protocol/Internet Protocol
USDA	-	United States Department of Agriculture
WWW	-	World Wide Web

5 POLICY

It is the policy of the United States Department of Agriculture to allow and encourage the use of Internet services to support the accomplishment of the various missions of the Department. Users of the Internet must be aware of the following policies regarding the content and management of Internet data and information.

a Acceptable Use

- (1) Federal Government telecommunication systems and equipment (including Government owned telephones, facsimile machines, electronic mail, interact systems (Internet), and commercial systems (when use is paid for by the Federal Government) shall be for official use and authorized purposes. (See GSA Federal Property Management Regulation (FPMR) 41 C.F.R. Subpart 101-35.1)
- (2) Authorized purposes may include limited personal use, with supervisor approval, and it is determined that such communications:
 - (a) Do not adversely affect the performance of official duties by the USDA employee or the USDA employee=s organization;
 - (b) Are of reasonable duration and frequency, and whenever possible, made during the USDA employee=s personal time such as after duty hours or lunch periods;
 - (c) Serve a legitimate public interest (such as educating the USDA employee on the use of the telecommunications system; enhancing the professional skills of the USDA employee; job searching in response to Federal Government downsizing);
 - (d) Do not put Federal Government telecommunications systems to uses that would reflect adversely on USDA or the Agency (such as uses involving pornography; playing on-line games; for purposes of private business; chain letters; unofficial advertising, soliciting or selling except on authorized bulletin boards established for such use; violations of statute or regulation; inappropriately handled sensitive information; and other uses that are incompatible with public service);
 - (e) Do not overburden the telecommunications system (such as may be the case with broadcasts and group mailings), and create no significant additional cost to USDA or to the Agency; and
 - (f) Follow the policy of the Internet Activities Board (IAB) as stated in RFC 1087.

b Privacy

- (1) USDA employees and contractors shall use Federal Government telecommunications systems with the understanding that such use serves as consent to monitoring of any type of use, including incidental and personal uses, whether authorized or unauthorized. In addition, access of

such systems is not anonymous. For example, for each use of the Internet over Federal Government systems, these systems may capture information transmitted, received or stored on the system. Additional information is available in the special instructions of the Main Body.

c Internet Uses

(1) USDA mission areas and staff offices may utilize the Internet to support departmental and mission area responsibilities. The Internet may be used for but is not limited to the following purposes:

- (a) The communication and exchange of data between state and local governments, private sector organizations, and educational and research institutions, both in the United States and abroad.
- (b) The development of Internet-based projects.
- (c) The balance of interactive sharing of information without compromising USDA secured data.
- (d) The exchange of any non-sensitive data between USDA entities in support of Departmental mission, agency missions, or other official purposes. Uses may include E-Mail and applications enabled by E-Mail.
- (e) For the distribution and collection of information related to official program delivery and in compliance with Federal and Departmental guidelines.

d USDA Internet Access Network

(1) The USDA Internet Access Network shall be used exclusively by USDA agencies and staff offices to connect to the Internet except in instances where a waiver to the use of the Internet Access Network has been granted by the Associate Chief Information Officer (CIO) for Policy.

- (a) The USDA Internet Access Network shall use FTS2000/2001 circuits to connect to the Internet and to transport inter-LATA data between USDA agencies and staff offices via the Internet.
- (b) A technical waiver shall be obtained from the Associate CIO for Policy, when an agency or staff office=s Internet access

requirements cannot be met by use of the USDA Internet Access Network. An Agency or staff office must meet the security requirements specified in DN 3140-5, or DR 3140-2, before the waiver is granted.

(c) An agency that currently accesses the Internet through a private Internet Service Provider (ISP) may continue such use, provided such use violates no mandatory Federal contract (e.g., FTS2000/2001) or other applicable Departmental Regulation, and provided the agency meets the security and cost justification requirements specified in DN 3140-5 or DR 3140-2 and obtains a technical waiver from the Associate CIO for Policy.

e Internet Protocol Addressing

(1) To access the Internet via the USDA Internet Access Network, an agency must use officially registered USDA IP addresses as explained in Appendix M, Internet Protocol (IP) Address Planning.

(2) Official IP addresses uniquely distinguish each host or device connected to the network. The Office of the Chief Information Officer (OCIO), Network Services Division (NSD) is the IP addressing and domain name registration authority for USDA.

(3) An agency shall not connect a host or other device that uses IP and has an unregistered IP address to the Internet, the USDA Internet Access Network, or to any network connected to either of these networks.

(4) Agencies and staff offices will modify their IP addressing plans to include the planned efficiencies and to bring all existing IP addresses into compliance with Appendix M, Internet Protocol (IP) Address Planning.

6 SECURITY

The connection of USDA hosts to the Internet increases the exposure of USDA systems to unauthorized access and abuse from the Internet. The Internet defines a host as any type of end-user computer system that connects to a network (e.g., personal computers, LAN servers, UNIX platforms, and mainframes, but not peripheral devices such as printers, plotters, or modems). Installation of firewalls and host-based security shall continue to be the primary methods for protecting those systems and remains the responsibility of the agency system administrators in accordance with applicable USDA (e.g., DR 3140-2) and agency regulations and guidelines.

a OCIO/NSD is receiving and redistributing the CERT Advisory Mailing List, ASSIST Security Bulletins, SUN Security Bulletins, the Firewalls-digest mailing list, and other information on Internet security as it is received from the Internet. This information is available from the USDA Internet Access Network's Security E-Mail list, Network Web (www.net.usda.gov) and Gopher (gopher.net.usda.gov) servers.

7 RESPONSIBILITIES

a Office of the Chief Information Officer will:

- (1) Provide appropriate oversight of USDA's use of the Internet, ensuring the USDA Internet Access Network provides a secure environment and is a cost effective service to the agencies; and
- (2) Provide customer support to agencies and staff offices regarding the use of the USDA Internet Access Network.

b Associate Chief Information Officer (CIO) for Policy will:

- (1) Process and respond to requests for technical waivers for separate access to the Internet for those agencies and staff offices that request waivers to the use of the USDA Internet Access Network.
 - (a) Analyze and review waiver documentation which includes obtaining technical waiver assurance that the USDA Internet Access Network cannot technically or cost effectively provide the capabilities requested and that the USDA Internet Access Network will not be negatively impacted;
 - (b) Review security documentation to ensure that agency verification of security controls provided by private ISPs is adequate;
 - (c) Maintain a data base of approved private ISPs used by agencies and staff offices in lieu of the USDA Access Network; and
 - (d) Annually review the data base for migration to the USDA Internet Access Network.
- (2) Perform vulnerability and risks assessments on agency network sites connecting to the USDA Internet Access Network.

c Office of the Chief Information Officer/Network Services Division will:

- (1) Process agency and staff office requests for IP network and subnetwork addresses and Autonomous System Numbers (ASN);
- (2) Refer all IP address service requests not received from an agency Point of Contact (POC) to the appropriate agency POC;
- (3) Maintain a complete inventory of officially registered USDA IP network and subnetwork addresses in use by agencies and staff offices;
- (4) Operate the primary name server for the USDA Internet Access Network;
- (5) Process agency requests for domain names and domain management. Request the allocation of domain names from GSA in the order of request receipt except domain names based on "<OFM/NFC agency name abbreviation>.usda.gov", which are reserved for the USDA agencies and staff offices;
- (6) Manage and maintain the Domain Name System (DNS)for USDA; including a complete inventory of officially registered domain names in use by the USDA agencies and staff offices;
- (7) Manage the DNS for any agency or staff office that requests a specific domain name but does not manage its own DNS;
- (8) Update and distribute the "Guide to the USDA Internet," when necessary;
- (9) Monitor usage of the Internet and maintain usage statistics; and
- (10) Ensure USDA Internet Access is protected by a firewall that meets requirements specified in DR 3140-2.

d Agencies and Staff Offices will:

1. IP Addresses

- (a) Designate a POC to coordinate requests for IP network and subnetwork addresses, domain names, ASNs, and technical waivers. Provide the POC's name, telephone number, postal address, and E-Mail address to OCIO/NSD and promptly notify OCIO/NSD when the POC's information changes. If multiple POCs are designated for a single agency, a description of each POC's scope of authority shall be included with the above information;

- (b) Request official IP network and subnetwork addresses, domain names, domain management, and ASNs from OCIO/NSD using the appropriate request forms;
2. USDA Internet Access Network Waivers
- (a) Designate an appropriate senior level manager who may be the Senior Information Resource Management Official (SIRMO) or the CIO to be the Certifying Official (CO);
 - (b) Require the CO to certify on behalf of the agency/staff office compliance with the requirements of this Departmental Regulation;
 - (c) Notify the OCIO of all uses of private IPSs within the agency/staff office. The CO shall provide the agency name (including subunit name, if appropriate), location, and supplier of the existing access, and a name and telephone number for a point of contact at the location for uses of private ISP=s not previously reported to the OCIO;
 - (d) Provide to the OCIO documentation signed by the CO certifying that a waiver has been requested and approved for each location using a private ISP and that required security controls are in place;
 - (e) Ensure that the Internet access in use does not create technical problems for the USDA Internet Access Network;
 - (f) Provide a compelling cost/benefit justification for the use of the private ISP;
 - (g) Include in requests for waivers to the use of the USDA Internet Access Network the following security information:
 - (1) A description of security controls in place protecting USDA information systems and data against unauthorized intrusion for each site;
 - (2) Documentation which defines security features available from each provider as well as a list of security features implemented;
 - (3) Documentation which specifically details each site=s compliance with DR 3140-2, National Institute of Standards and Technology (NIST) Special Publication 800-

12, NIST Special Publication 800-14, and Office of Management and Budget (OMB) Circular A-130, Appendix III, dated February 6, 1996; and

(4) OMB 90-08 Agency Security Plan reflecting the inclusion of provisions stated in Section d, subpart 2g (1)-(4).

(h) Conform to the requirements of OMB Circular A-119, when applicable.

8 FORMS

Forms for requesting various types of Internet access and services are described below. Electronic versions of the forms may be obtained from the USDA Internet Access Network's Web (www.net.usda.gov) and Gopher (gopher.net.usda.gov) servers, or by sending a request to OCIO/TSO.

a Other services, as specified in the "Guide to the USDA Internet," may be requested utilizing the appropriate form which is available as indicated above.

b An IP Subnetwork Address may be requested by providing the information indicated on the IP Subnetwork Address Request Form.

c A USDA Domain Name may be requested by providing the information indicated on the USDA Domain Name Request Form.

d Management of a USDA Domain may be requested by providing the information indicated on the USDA Domain Management Request Form.

9 DEFINITIONS

a Access Network Router. The router which joins the USDA Internet Access Network to an agency private network.

b Agency Private Network. A network used solely by a single agency or agency subunit. An example of such a network would be a local area network that serves a single subunit of a particular agency.

c Autonomous System Number. A unique 16 bit number assigned by the InterNIC that refers to a particular collection of networks under a common administration and sharing a common routing strategy. Soon USDA will begin

using the Border Gateway Protocol between the two Department-wide access points and the Internet and begin advertising the USDA Internet Access Network as one Autonomous System (AS). This configuration will give USDA the capability to automatically reroute traffic when either access point goes down. OCIO/NSD will administer ASNs for USDA.

d Domain. A defined set of applications, systems, users, or organizations interrelated by virtue of being administered by a common authority.

e Domain Name System. A distributed database system established by the Internet to enable the translation of alphabetic (user friendly) domain names into numeric (machine friendly) IP addresses and vice-versa. Several root, or first level, domains have been established, such as "mil" for DOD, "edu" for universities, and "gov" for federal government entities.

f InterLATA. As applied to FTS2000/2001 network services, a telecommunications transmission between two or more locations that are in different Local Access and Transport Areas.

g Internet. A collection of thousands of networks linked by a common set of technical protocols which make it possible for the users of any one of the networks to communicate with or use the services located on any of the other networks. These protocols are referred to as the TCP/IP protocol suite. It is the world's largest interconnected network of networks consisting of a national backbone and a myriad of regional and local networks connecting primarily colleges, universities, and government organizations (such as the National Science Foundation (NSF) and the Advanced Research Projects Agency (ARPA)).

h Internet Protocol. The network layer protocol for the Internet protocol suite that allows the interconnection of multiple networks and uses information such as a globally unique Internet source and destination address to route packets from one network to another.

i IP Address. An IP address is a 32-bit number that is intended to uniquely identify each host or device that is connected to the network. IP addresses are normally allocated in groups known as network or subnetwork addresses.

j USDA Internet Access Network. USDA access to the Internet gateways is currently in the Washington, D.C. metropolitan area and Fort Collins, CO and is provided via the USDA Internet Access Network. The USDA Internet Access Network is a logical scalable network that coexists with other logical networks and will serve the Internet Access component for a USDA Enterprise Network. A USDA Enterprise Network will be owned, managed, and operated by the USDA and use FTS2000/2001 circuitry for all interLATA transport of data, including E-Mail, applications enabled by E-Mail, and data exchanges.

