U.S. Department of Agriculture

Washington, D.C. 20250

DEPARTMENTAL REGULATION	Number: 3140-002
SUBJECT: USDA Internet Security Policy	DATE: March 7, 1995 OOPI: Office of Information Resources Management, Agency Technical Services Division

1 PURPOSE

This regulation establishes minimum security requirements for the use of the Internet network by U. S. Department of Agriculture (USDA). This regulation is not written to restrict the use of Internet, but to ensure that adequate protection is in place to protect USDA data from intruders, file tampering, break in, and service disruption.

2 BACKGROUND

In the late 1960s the Department of Defense (DoD) designed and implemented the ARPAnet network for the exchange of defense industry research information world-wide. TCP/IP was the protocol developed and UNIX was the platform.

The National Science Foundation (NSF) needed a network also to interconnect their supercomputers and exchange academic research information so they built their own, but followed the DoD standards. They called their network NSFNET.

The Internet consists of many, worldwide, independent networks that allow interconnection and transmission of data across the networks because they follow the same basic standards and protocols and agreed upon Internet etiquette, " No central authority." Each user organization pays for its own piece of the network.

Motivated by developments in highspeed networking technology and the National Research and Education Network (NREN) Program, many organizations and individuals are looking at the Internet as a means for expanding their research interests and communications. Consequently, the Internet is now growing faster than any telecommunications system thus far, including the telephone system.

New users of the Internet may fail to realize, however, that their sites could be at risk to intruders who use the Internet as a means for attacking systems and causing various forms of threat. Consequently, new Internet sites are often prime targets for malicious activity including break in, file tampering, and service disruptions. Such activity may be difficult to discover and correct, may be highly embarrassing to the organization, and can be very costly in terms of lost productivity and compromised data integrity.

All Internet users need to be aware of the high potential for threat from the Internet and the steps they should take to secure their sites. Many tools and techniques now exist to provide sites with a higher level of assurance and protection.

USDA agencies should acquire a copy of the "Guide to the USDA Internet." This document is published by the Office of Information Resources Management. This guide defines the USDA Internet Access Network. You may acquire this guide by contacting the Director, Office of Information Resources Management, room 414-W.

3 DEFINITIONS

Definitions relating to this policy may be found in appendix "A".

4 REFERENCES

NIST CSL Bulletin, July 1993, NIST Connecting to the Internet: Security Considerations

NIST CSL Bulletin, May 1994, NIST Reducing the Risks of Internet Consideration and use

NIST Publication, Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls (Draft) September 1994,

USDA OIRM, DR 3140-1, USDA IRM Security Policy Dated March, 1995

USDA OIRM, DR 3300-1, Telecommunications (Appendix I, Internet), dated April 8, 1994

USDA OIRM, Guide to the USDA Internet

5 ABBREVIATIONS

ARPAnet	Advanced Research Projects Agency Network
DMZ	Demilitarized Zone
DoD	Department of Defense
FTP	File Transfer Protocol
IRM	Information Resources Management

ISPM	Information Security Program Manager
LAN	Local Area Network
NIST	National Institute of Standards and Technology
NSF	National Science Foundation
NFS	Network File System
NREN	National Research and Education Network
OIRM	Office of Information Resources Management
OMB	Office of Management and Budget
OSI	Open System Interconnect
TCP/IP	Transmission Control Protocol/Internet Protocol
TCP	Transmission Control Protocol
USDA	U.S. Department of Agriculture

6 POLICY

The responsibility for protecting USDA resources on the Internet is the responsibility of the USDA Agencies or Staff Offices. This policy apply to contractors and universities that connect to USDA computer. USDA agencies which access the Internet must develop and implement an Internet security policy which meets the minimum requirements of this regulation as following:

a Data which is exempted from disclosure under the Freedom of Information Act (Public Law 93-502) or whose disclosure is forbidden by the Privacy Act (Public Law 93-579) will not be transmitted over the Internet network unless encrypted. "Note: Logon IDs and passwords are frequently classified as sensitive information."

b All USDA agencies and staff offices using the Internet must follow the guidance in DR 3300-1 "Telecommunications," and report to OIRM the information requested in Appendix I, Section 4.

c USDA agencies and staff offices that plan a gateway to the Internet are responsible for funding, implementing and maintaining the prescribed protection, including devising, and implementing a comprehensive risk management program.

d Agencies and staff offices will access the Internet only through the USDA Internet Access Network. Any agencies currently accessing the Internet through other means may continue to do so provided:

(1) No other mandatory Federal contract (e.g., FTS2000) or Departmental Regulation is violated; and

(2) The agency has submitted and obtained approval of a technical waiver request registering the use to the Director, Office of Information Resources Management.

e Host-based security will be the primary method of protecting USDA systems. However, many host-based security software packages cannot be trusted to protect us from the Internet, because of their vulnerability to denial-of-service attacks.

f Due to inherent weaknesses in certain Internet telecommunication services, and cumbersome aspects of some security packages, many sites will find that the most practical method of securing access to systems from the Internet is to use a secure Gateway or a firewall system. Agencies will perform risk assessments to determine where secure gateways, firewalls, smart cards, or authentication tokens will be most suitable. USDA agencies will:

(1) Use firewalls and/or packet filters on the local routers, when the system uses TCP/IP.

(2) Configure firewalls on with outgoing access to the Internet, but strictly limit incoming access to USDA data and systems by Internet users.

(3) Apply the DMZ concept as part of the firewall design.

g Firewall compromise would be potentially disastrous to subnet security. For this reason, agencies will, as far as is practical, adhere to the below listed stipulations when configuring and using firewalls.

(1) Limit firewall accounts to only those absolutely necessary, such as the administrator. If practical, disable network logins.

(2) Use smartcard or authentication tokens to provide a much higher degree of security than that provided by simple passwords. Challenge-response and one-time password cards are easily integrated with most popular systems.

(3) Remove compilers, editors, and other program development tools from the firewall

system(s) that could enable a cracker to install Trojan horse software or backdoors.

(4) Do not run any vulnerable protocols on the firewall such as TFTP, NIS, NFS, UUCP.

(5) Consider disabling finger command. The finger command can be used to leak valuable user information.

(6) Consider not using the e-mail gateway commands (EXPN and VFRY) which can be used by crackers to probe for user addresses.

(7) Do not permit loopholes in firewall systems to allow friendly systems or users special entrance access. The firewall should not view any attempt to gain access to the computers behind the firewall as friendly.

(8) Disable any feature of the firewall that is not needed, including other network access, user shells, applications, and so forth.

(9) Turn on full-logging at the firewall and read the logs weekly at a minimum.

h No USDA computer or subnet that has connections to the Internet can house privacy or sensitive information without the use of firewalls or some other means to protect the information.

i USDA agencies and staff offices must develop and document an Internet security strategy based on the type of Internet service selected for use. This strategy must be included in the Internet Security Plan.

j USDA agencies and staff offices that use the Internet must adhere to guidance stated in DR 3140-1 "USDA IRM Security Policy."

k All software available on the Internet must be scanned for Trojan horses or computer viruses once it has been downloaded to a USDA computer. All downloaded software should be loaded preferably onto a floppy disk and not to the system hard disk. Once you are reasonably assured that the downloaded software does not contain Trojan horses or computer viruses it can be placed on the hard drive. If the software will not fit on a floppy disk then the only option is the hard disk. The software must be scanned before use (executed).

l Mandatory vulnerability and risk assessment of existing gateways is required at annual intervals. Initial assessment should be completed within nine (9) months of the issuance of this policy.

m Agencies should conduct weekly or monthly reviews of audit trails of gateway software for breaches of security.

n USDA personnel, and contractor personnel working for USDA while using the Internet:

(1) Must not be harassing, libelous, or disruptive to others while connected to the Internet.

(2) Must not transmit personal data or unauthorized government-owned data across the internet.

(3) Must obey all copyright laws.

(4) Must not download to government computers from the Internet any obscene written material or pornography.

(5) Must not send threatening, racially harassing, or sexually harassing messages.

(6) Must not attempt to break into any computer whether USDA, federal or private.

(7) Must not be used for private or personal business.

(8) Must not introduce computer viruses, worms, or Trojan horses.

o USDA sponsored Internet connections are to be used for official USDA business.

p Host computers should be regularly scanned to ensure compliance with USDA security guidelines.

7 RESPONSIBILITIES

a The Director, OIRM, will:

(1) Develop, coordinate, implement, interpret, and maintain Internet Security policies, procedures, and guidelines for the protection of USDA information system resources.

(2) Review agency Internet security policy.

(3) Assist in agency Internet security policy development.

(4) Determine adequacy of security measures for systems used as gateways to the Internet.

(5) Ensure that agencies conduct periodic information systems security risk assessments, security evaluations, and internal control reviews of operational USDA Internet gateways and facilities.

b Agencies and Staff Offices That Have or Are Planning a Gateway to the Internet will:

(1) Devise and implement a comprehensive risk management program which assures that security risks are identified, considered, and mitigated through the development of cost effective security controls. The risk management system will include a service access policy that will define those services that will be allowed or explicitly denied from the restricted network, how these services will be used, and the conditions for exception to this policy.

Another part of this risk management system will be a firewall design policy. This policy relates precisely to firewalls and defines the rules used to implement the service access policy.

Each agency and staff office must develop an Internet Security Plan which address all security controls in place or planned. These controls shall be commensurate with the risks identified in the risk analysis. Internet Security plans shall be submitted annually with the IRM Security Plans for review and approval. The guidelines governing the submission of IRM Security Plans as defined in DR- 3140-1 apply to the submission the Internet Security Plan.

(2) Perform risk analysis to identify the risks associated with using Internet both for individual users and Agency or Staff Office. Cost effective safeguards, identified in the risk analysis process, will be implemented and continually monitored to ensure continued effectiveness.

(3) Develop, test, and maintain Internet contingency plans. The risk involved with using the Internet makes it essential that plans and procedures be prepared and maintained to:

(a) Minimize the damage and disruption caused by undesirable events; and

(b) Provide for the continued performance of essential systems functions and services.

(4) Develop, install, maintain, and regularly review audit trails for unusual system activity.

(5) Fund, implement, and maintain the prescribed protective features identified as a solution by a risk assessment.

(6) Risk assessment developed by agencies and staff offices are to be made available to OIRM upon request.

(7) Ensure that the agency Information Security Program Manager is a vital part of any security activity on the Internet.

c Agency Information Security Program Manager is responsible for:

(1) Implementing the policy stated in this directive.

(2) Developing audit trails for any USDA network connected to the Internet.

(3) Reviewing and monitoring activity audit trails on the Internet connections.

(4) Working closely with the agency network administrator in monitoring activity on the use of their host and subnets.

8 NON-COMPLIANCE

All users of data and systems are responsible for complying with this Internet systems security policy, as well as procedures and practices developed in support of this policy.

Anyone suspecting misuse or attempted misuse of Departmental information systems resources is responsible for reporting such activity to their Agency or Staff Office management, or to the Information System Security Program Manager or the Departmental Information System Security Program Manager.

Violations of standards, procedures, or practices in support of this policy will be brought to the attention of management for action, which will result in disciplinary action up to and including termination of employment.

9 SOURCE OF INFORMATION

a OIRM, Guide To The USDA Internet

b The following source documents may be obtained through the NIST Bulletin Board Service (BBS). To access the BBS, you need a computer with communications capability and a modem. For modems at 2400 bits per second (BPS) or less, dial (301) 948-5717. For 9600 BPS, dial (301) 948-5140. Modem settings for all speeds are 8 data bits, no parity, 1 stop bit.

(1) CSL Bulletin, July 1993, NIST Connecting to the Internet: Security Considerations

(2) CSL Bulletin, May 1994, NIST Reducing the Risks of Internet Consideration and use

(3) NIST Publication, September, 1994 Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls (Draft)

c Internet users with telnet or ftp capability may telnet to the BBS at cs-bbs.nist.gov (129.6.54.30). To download files, users need to use ftp as follows: ftp to csrc.nist.gov (129.6.54. 1 1), log into account anonymous, use your Internet address as the password, and locate files in directory pub; an index of all files is available for download. For users with Internet-accessible e-mail capability, send e-mail to docserver@csrc.nist.gov with the following message: send filename, where filename is the name of the file you wish to retrieve. Send index will return an index of available files.

d Hard copy of NIST publications can be obtained by contacting National Institute of Standards and Technology at the following address:

NIST, Building 225

Room A-216

Gaithersburg, Maryland 20899-0001

Telephone No. (301) 975-3359

Fax No. (301) 948-0279

Sign by:

DAVID R. SKEEN

APPENDIX A

DEFINITIONS

Application Protocol. Protocol used by applications that are invoked by the user (example: E-mail).

Backdoor. A term used to describe an entry to a network or computer. Usually a hidden logon identification (ID) and password are used to gain access through the backdoor. The hidden logon ID and passwords may be placed on the system by a hardware or software manufacture as a way for their technician to gain access for repair. Computer hackers/crackers may use these hidden logon IDs and passwords or use trojan horses to establish illegal and unauthorized logon IDs and passwords on systems. These IDs and passwords become the backdoor entry point to the computer system or network. The main illegal use of backdoors is to get around computer system or network security.

Computer Crackers. A name given by computer hackers to persons who break into systems and abuse the systems they break into. No matter what name is used, the unauthorized access of computers by the computer hacker or the cracker is a criminal act by law.

Computer Hacker. A person or group of persons using computers to illegally break into other computers. These persons normally have interest only in the ability to break into another system. This term also describes computer "whiz kids" who push their knowledge of computers and programming to its limits. The unauthorized access of computers by the computer hacker is a criminal act by law.

Computer Virus. A program designed to infect computer systems in much the same way as a biological virus infects humans. The typical virus reproduces by making copies of itself when inserted into other programs. Computer viruses normally infect either systems software or application programs.

Demilitarized Zone (DMZ). A screened "sub-net" configured such that both the Internet and the private network have access to hosts on the screened subnet, but traffic across the screened "subnet" is blocked. The subnet network is setup between the private "protected" network and the Internet [so that] to all hosts on the "subnet" are reachable from the outside."

Finger Command. A command which displays information about a user. This command will also display the contents of a file named in the users home directory.

Firewalls. An approach to security; it is a policy that defines the services and access to be permitted, and an implementation of that policy in terms of a network configuration, one or more host systems and routers, and other security measures such as advanced authentication in place of static passwords. The main purpose of a firewall system is to restrict access to or from a protected network (i.e., a site). It implements a network access policy by forcing connections to pass through the firewall, where they can be examined and evaluated.

Logic Bomb. A computer code that is preset to cause a malfunction when a specified set of logical conditions occur. For example, when a specific social security number in a payroll system is processed, the logic bomb is activated. The logic bomb will then cause an improper amount of money to be printed on the check.

Network File System (NFS). A system that allows you to work with files on a remote host as if you were working on your own host.

Network Information Services. Allows multiple systems to share databases, e.g., the password file, to permit centralized management.

Internet. A collection of world-wide "network of networks" that use the TCP/IP protocol suite for communications.

Internet Subnet. A USDA owned network which has been connected to the Internet.

Packet Filters. A router designed to screen packets as they pass between the router's interfaces. Filtering can be used to block connections from or to a specific host or network, and to block connections to specific ports.

Protocol. A set of rules that defines how computers transmit information to each other, allowing different types of computers and software to communicate with each other.

Router. A system used to transmit data between two computer systems or networks using the same protocol.

Risk Assessment. A process which analyzes and identifies current system value assets, existing security safeguards, vulnerabilities and determines impacts associated with an automated system or network. The risk assessment also identifies potential security safeguards.

Scan. A method used to examine computer coding/programs sequentially, part by part. Scans are made for virus signatures or potentially unsafe practices. (For example: scan for changes made to an executable file, or search for direct writes to specific disk sectors, etc.)

Sensitive Information. Information for which loss, unauthorized modification, or unauthorized disclosure would be detrimental to agency operations. Examples: information that is personal, proprietary, financial, National Security-related, or critical to agency plans and operations.

Shareware. Software that has been developed and placed in public domain or in general circulation for general public use. The developer of this software may requests a small fee ($1.00 - $20.00) for use and future updates.

Spoofing. A method of tricking system security into permitting normally disallowed network connections.

Subnet Security. Security provided at the USDA agency level network which has been connected to the Internet.

TCP/IP Protocol. A suite of rules (protocols) that define how data is transported among computers on the Internet.

Time Bomb. A computer code that is preset to cause a malfunction after a specific date, time, or number of operations. The "Friday the 13th" computer virus is an example. The system is infected for several days, or even months, and the virus lies dormant until the date reaches "Friday the 13th."

Trap Door. A set of instruction codes embedded in a computer operating system that permits access while bypassing security controls.

Trojan Horse. A set of unwanted embedded computer instructions inside a program. The instructions cause unexpected results when the program is executed. It may create logon ID's and passwords for later intrusion by hackers. Further, Trojan horses allow persons to create or gain access to the source code of common or frequently used programs. These programs may be modified to perform a harmful function in addition to its normal function. A Trojan horse can alter, destroy, disclose data, or delete files.

Virus Detection Software. Software written to scan machine readable media on computer systems. There are a growing number of reputable software packages available that are designed to detect and/or remove viruses. In addition, virus checkers programs can search text files for virus signatures or potentially unsafe practices.

Virus Signature. A unique set of characters which identify a particular virus. This may also be referred to as a virus marker.

Worm. A complete program that propagates itself from system to system, usually through a network or other communication facility. A worm is similar to a virus and can infect other systems and programs. A worm differs from a virus in that a virus replicates itself, and a worm does not. A worm copies itself to a person's workstation over a network or through a host computer and then spreads to other workstations. It can easily take over a network as the "Internet" worm did. Unlike a Trojan horse, a worm enters a system uninvited.

TFTP. A protocol used for booting diskless workstations, terminal servers and routers.

Unix. A computer operating system developed by Bell Laboratories. This system was developed originally for Bell Laboratories' internal use. The computer world learned of its portability and the system expanded into universal use. Unix runs on a variety of computer hardware.

USDA Internet. Is comprised of an interconnection of networks "owned" and operated by the USDA. It is not the same as "The Internet"; however it relies upon "The Internet" to interconnect with many other important networks. The USDA Internet uses FTS2000 circuits and The Internet does not use FTS2000 facilities. This is an important distinction since FTS2000 mandates the USDA use network 'A' circuits whenever intra-USDA business is conducted across Local Access and Transport Areas.... [The USDA Internet] is not a public network. [Nor is it a] network which comprises the core of the Internet [like some networks such as NSFNet]."

UUCP. Unix-to-Unix copy protocol. A system by which files can be transferred between Unix computers.

UUCP network. A network of Unix computers sites, that communicates via modems and phone lines using the UUCP protocol.

END