CHAPTER 5, PART 2
INTERNET USE & COPYRIGHT RESTRICTIONS

1 BACKGROUND

The proliferation of the Internet as a working tool in USDA has necessitated that security measures for its use be more clearly defined. This has been highlighted by the results of Intrusion Detection Scans (IDS) of networks and firewalls nationwide. During these scans, Cyber Security has detected increased activity in areas that users should know are unauthorized.

Scans of department Internet Protocol (IP) addresses have identified users engaging in the download of programs that enable the user to subsequently download other software, music, graphics or videos, including pornographic materials; in some instances, this material is downloaded and distributed to others. These users are using a number of Peer-to-Peer (P2P) programs and “file sharing” products available for download from the Internet. Some of the products detected include: gnutella, LimeWire, SwapNut, KaZaA, and Morpheus. These “evasive” programs have the ability to send inbound and outbound traffic to regular Internet ports for transport, thus disguising their purpose.

Removing these programs from Government equipment causes undue departmental expense and can involve days of effort. Repeated and continuous use of this type of software can impact network resources and inhibit USDA’s ability to properly discharge our mission. Software downloads have been detected independent of the use of P2P programs and the like. As indicated above, the fact that special programming is not involved in downloading these materials does not alter the possible criminal nature of distributing pornographic material to others. In addition, copyright infringement may exist if the material being downloaded found its way onto the Internet without the owner’s permission, or if the user employs the downloaded material contrary to instructions therewith.

2 POLICY

USDA has a long established policy that does not condone or support employees use of Government computers or networks for unauthorized purposes. P2P Programs and other programs that perform those functions have no recognized departmental business need and should not be loaded on workstations or equipment used to conduct USDA Official Business without an approved exception from the Associate CIO for Cyber Security. Specifically, USDA employees are prohibited from loading P2P software on USDA equipment, downloading illegal material, downloading copyrighted material for personal use, and the distribution of illegally obtained files and software. The "Limited Personal Use Policy" defined in DR 3300-1 cannot be used as a justification for downloading P2P or other programs that perform those functions, downloading or distributing pornographic material or copyright infringement.

Agencies must apply this policy to all personnel that use USDA equipment, facilities, including USDA telecommunications, and Internet access networks, or perform services for or on behalf of USDA. Agencies have no authority to allow these groups to use Government equipment for these unauthorized activities improperly or to charge the Government for these unauthorized activities.

Each agency will establish an electronic system to monitor Internet usage by all personnel using USDA equipment to ensure that they adhere to these requirements in the performance of their official duties and while using USDA computers and networks. This system should be designed to monitor each website a user accesses but not be keystroke monitoring. For accountability reasons, each agency and mission area will be able to electronically identify all IP addresses to specific users. Each agency is required to provide warning banners to users advising them of the intent to monitor USDA network, systems and equipment, making specific reference to the unauthorized activities and notifying users that the use of the computer system and network is an expression of consent to such monitoring. All agencies and mission areas are responsible for enforcing this policy to protect USDA Information Technology (IT) resources and for providing security awareness training on an annual basis.

Agencies will refer instances of pornography to the Office of the Inspector General (OIG) and will respond to requests from CS for follow up action on instances of unauthorized use. They will coordinate all necessary investigative and follow up actions with the OIG, law enforcement and appropriate agency Office of Human Resources Management (HRM).

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 RESPONSIBILITIES

a The Chief Information Officer and Deputy will:

Support and enforce this policy throughout all of USDA and actively coordinate with law enforcement and agency activities to ensure that employees and other groups use the Internet to conduct authorized activities.

b The Associate CIO for Cyber Security will:

(1) Perform continuous scans of all USDA networks and systems to detect unauthorized activity by employees, contractors, subcontractors, grantees and cooperators;

(2) Analyze closely the results of these scans and take remedial action with the agency and mission area to ensure that :

(a) Instances of pornography are forwarded to the Office of Inspector General (OIG);
(b) Instances of child pornography are forwarded to the appropriate law enforcement office;
(c) Instances of unauthorized use are forwarded to the agency and mission area for review, appropriate follow-up and administrative action;

(3) Actively support each agency and mission area in the resolution of all instances of unauthorized use of the Internet;

(4) Actively provide assistance to the OIG, law enforcement offices, and agency Human Resource Management offices in the investigation of all parties violating this policy;

(5) Maintain an electronic record of all instances of unauthorized use of USDA equipment, networks and systems to support prosecution or administrative action requirements;

(6) Ensure through audits that each agency and mission area complies with the requirements of this policy to include modification of warning banners to advise users of unauthorized activities and the USDA's intent to monitor all networks, systems and equipment;

(7) Collaborate with agencies and mission areas in conducting training and awareness programs designed to inform all USDA users of the appropriate use of the Internet, networks, systems and equipment;

(8) Collaborate with the Office of Procurement and

Property Management to ensure that guidance (AGAR Advisory) is issued to the procurement community advising them of the need to incorporate this policy in all new contracts; and

(9) Ensure that agency program offices preparing procurement requests, including statements of work, and specifications, incorporate a requirement that contractors and subcontractors comply with this policy;

c <u>The Associate CIO for Information Resources Management will:</u>

(1) Support the policy and procedures contained in this chapter 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 for exceptions to this policy.

d <u>The Office of Inspector General will:</u>

(1) Respond to all instances of unauthorized use of the Internet or USDA networks, systems and equipment by working with Cyber Security to take the appropriate remedial action to include prosecution or administrative action;

(2) Promptly initiate investigations, where deemed appropriate, to protect USDA IT resources or advise Cyber Security that administrative action is warranted by the agency or mission area;

(3) Collaborate with agencies and mission areas to ensure appropriate administrative action is being taken; and

(4) Conduct routine audits on agency and mission areas Internet use, Warning Banners, training and awareness programs and monitoring systems to determine compliance with this policy and procedures.

e The Office of the Chief Financial Officer will:

Issue Department-wide guidance applicable to assistance grants and cooperative agreements to reflect the requirements of this policy and procedures to prevent unauthorized use of the Internet or USDA Information Technology resources by grantees and cooperators;

f Agency Chief Information Officer will:

(1) Ensure that the policy and procedures in this Chapter are implemented in all areas for which they are responsible;

(2) Coordinate with acquisition activities to modify existing contracts, as necessary, to apply this policy to all USDA contractors, subcontractors, grantees and cooperators that use USDA equipment and facilities, including telecommunications and Internet access networks, or perform services for or on behalf of USDA;

(3) Ensure a system is established to monitor Internet usage by all employees, contractors, subcontractors, grantees, and cooperators using USDA equipment to ensure that they adhere to the requirements of this policy during the performance of their official duties and while using USDA networks and systems; this system should be designed to monitor each Web site that a user accesses (audit trail) but should not include keystroke monitoring;

(4) Ensure that agency programs assign one IP address per user or be able to identify dynamically assigned addresses to individual users;

(5) Ensure that all agency/mission area Warning Banners are revised to make specific reference to the above-described unauthorized activities, and to include notice that there will be periodic and routine monitoring of Internet usage and that the user expresses consent to such monitoring through his or her use of USDA computer systems or networks;

(6) Provide oversight to ensure that computer security awareness and training is conducted for all users in the authorized use of the Internet and all IT resources;

(7) Ensure that necessary action is taken to report all instances of unauthorized use of the Internet and USDA IT resources, and cooperate with the OIG, law enforcement and Human Resource Officials during investigations and any subsequent legal or administrative proceedings; and

(8) Ensure that language is included in all new Statements of Work, specifications and procurement/grant/cooperative agreement requirements that require compliance with this policy by contractors, subcontractors, grantees and cooperators.

g <u>Agency Information Systems Security Program Managers or designate will:</u>

(1) Assist the system and network administrators in monitoring Internet use by agency employees, contractors and subcontractors;

(2) In coordination with the SA ensure that agency Warning Banners are updated to: make specific reference to unauthorized Internet activities; to include notice concerning periodic and routine monitoring of Internet use; and that the user

expresses consent to such monitoring through his or her use of USDA computer systems and networks;

(3) Electronically identify and monitor incidents of policy violations and report such incidents to Cyber Security in accordance with the USDA Computer Incident Response Procedures;

(4) Assist the OIG and law enforcement offices in collecting investigative and forensic evidence as required;

(5) Secure all investigative and forensic data in a locked cabinet in accordance with the USDA Computer Incident Response Procedures; and

(6) Conduct security awareness training for all agency and mission area employees and contractors with a focus on authorized Internet use and appropriate use of USDA systems, networks and equipment.

h Agency System and Network Administrators and Webmasters will:

(1) Monitor all agency Internet usage by all authorized users; assign one IP address per user;

(2) Coordinate all instances of unauthorized activities with the agency ISSPM or designate;

(3) Update all agency computer Warning Banners with language meeting the requirements outlined above; and

(4) Assist, as required, in collecting investigative and forensic data for cases under investigation by the OIG or law enforcement offices.

- END -