

CHAPTER 3 -PART 1 COLLECTION OF WEB PAGE COOKIES & PRIVACY REQUIREMENTS

1 BACKGROUND

The free flow of information between the government and the public is essential in a democratic society. However, the individual's right to privacy must be protected in the Federal Government information activities involving personal information. On June 2, 1999, the OMB directed that USDA post clear privacy policies on our Internet and Intranet Web sites. Subsequently, on June 22, 2000, OMB refined this requirement to include any contractor operating Federal Web sites on behalf of the Federal Government. USDA's Privacy Policy specifies that we will collect no personal information about visitors to our Web sites. This policy requires that each Web site clearly and concisely inform visitors what information the agency collects about individuals, why the agency collects it and how the agency uses it. This includes a responsibility to protect the privacy of individuals accessing USDA Web sites. On November 15, 2000, OCIO published guidance on the collection and use of cookies on all USDA Internet and Intranet Web sites. Overall questions regarding this policy should be directed to the USDA Office of the Chief Information Officer, Office of Cyber Security.

2 POLICY

This manual requires that agencies collect or create only that information necessary for the proper performance of agency functions and which has practical utility. Each agency/mission area will consider the effects of their actions on the privacy rights of individuals, and ensure that appropriate legal and technical safeguards are implemented.

Agencies must exercise care to ensure that they comply with OMB's privacy policies cited in the Reference Section and the requirements outlined in the Privacy Act, (5 USC 552a). As a reminder, the Privacy Act covers information about individuals that is retrieved by reference to a personal identifier. The definitions of an "individual" and "record" are outlined in Part 1, Section 4 of this chapter.

Specifically, USDA Web sites operated by agency personnel or contractors on behalf of agency/mission areas may not use "cookies" or "agents" to acquire and track personal information or web browsing habits unless specifically approved by a exception signed by the Secretary of USDA. There are two types of cookies or web agents: a session cookie and a persistent cookie. General Information, Section 6, Definitions, contains an explanation of these terms. Persistent cookies may not be sent to visitors to Web sites except under the conditions for a exception outlined below.

Visitors will receive clear and concise information concerning what information is collected on individuals and how it is used. Agencies will comply with the standards set forth in the Children's Online Privacy Protection Act of 1998 with respect to the collection of personal information at Web sites directed at children. No agency/mission area will collect personal information about individuals when they visit our websites unless the visitor chooses to provide that information. If the individual provides personal information, in E-mail or by filling out a form, USDA agencies will only use that information to respond to the message or to serve the need of the individual, except to the extent that the information is properly incorporated into an agency's system of records in which case the information will be stored and used in accordance with the Privacy Act. This provision does not apply to E-mails that are the subject of an investigation by the Office of the Inspector General (OIG) or other law enforcement activities.

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. The Secretary of Agriculture is the only person authorized to approve exceptions.

3 RESPONSIBILITIES

a The Chief Information Officer or Deputy CIO will:

Ensure that USDA agencies/mission areas and contractors comply with the requirements of the Privacy Act and the Children's Online Privacy Protection Act of 1998 with regard to the collection and use of personal information.

b The Associate CIO for Cyber Security will:

- (1) Require that visitors to all USDA Web sites receive a conspicuous USDA privacy notice policy statement upon entering all sites;
- (2) Publish guidance that prohibits the collection and use of persistent "cookies" or "Web agents" by agencies and contractors operating USDA Web sites without an approved exception signed by the Secretary USDA;
- (3) Monitor and verify that all USDA Web sites comply with the requirements of the Privacy Act and the Children's Online Privacy Protection Act of 1998 with regard to the collection and use of personal information;
- (4) Review all persistent cookie exception requests submitted by USDA activities where cookies would obtain personal data to ensure that the rights of the individual are not compromised for less than compelling business needs;
- (5) Issue direction to cease operating Web sites if the agency/mission area or contractor is not in compliance with the privacy policy/procedures in this manual and does not correct the problem in a timely manner (12 hours); and

- (6) Maintain a current USDA Web site inventory to include a list of Web sites with approved exceptions to collect privacy information.

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

- (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 to this policy.

d The Department Information Systems Security Program Manager (ISSPM) will:

- (1) Maintain a current electronic list of all official USDA Web sites that include Point of Contact information;
- (2) Conduct periodic reviews of Web sites, as part of overall security compliance, to ensure that USDA agencies/contractors are not collecting and using "persistent cookies" or Web agents" and that sites are providing notice of USDA's Privacy Policy to visitors; and
- (3) Promptly notify the Associate CIO for Cyber Security of any Web site that does not comply with the Privacy requirements.

e The Office of the Inspector General will:

Incorporate, as appropriate, into audits of USDA Web sites a review of applicable requirements Concerning the collection/use of persistent Cookies and posting of privacy notices.

f Agency Management and Information Technology Officials or Chief Information Officer will:

- (1) Establish and implement internal procedures that

prohibit the collection and use of persistent “cookies” on all agency Web sites and applications hosted by USDA Web servers or servers used by contractors to host USDA Web sites unless approval has been received in writing from the Secretary USDA;

- (2) Ensure that all agency Internet and Intranet Web sites are inventoried to include Point of Contact Information; update this list monthly and provide a copy of the inventory list to the Associate CIO for Cyber Security;
- (3) Assure that all agency Web sites provide clear and concise notice of USDA’s Privacy Policy concerning individuals and children;
- (4) Prepare exceptions for exceptions to this policy only when a compelling business need justifies the collection of information on individuals; all exception requests will be signed by the agency CIO/IT Manager and contain assurances concerning the protection of this information; and
- (5) Ensure that all agency Program Managers, IT personnel and contractors are aware of the requirements of this policy in connection with the daily operation of agency Internet and Intranet sites.

g The agency/mission area Information Systems Security Program Manager (ISSPM) will:

- (1) Prepare and maintain a complete inventory list of all agency Internet and Intranet Web sites; this list will include Point of Contact information (Name, Phone, Location, E-mail address) for each Web site;
- (2) Provide a copy of the Web site inventory list to the Department ISSPM and update monthly or as changes occur; and
- (3) In coordination with the agency Systems Administrator/Web Master, ensure that all agency/mission area servers have been optioned to send only session cookie text to individuals accessing

agency web sites. In addition, the ISSPM will ensure that clear privacy notices have been posted to Web sites to advise visitors, including children, of USDA's Privacy Policy.

h The agency Systems Administrator/Web Master will:

- (1) If cookies are required, option all agency Web servers to send only "session cookies" to visitors accessing USDA Web sites, unless the Secretary of Agriculture has approved an exception in writing;
- (2) Ensure that all Web sites provide clear and conspicuous notice to all visitors, including children, of USDA's Privacy Policy in compliance with the requirements of this manual; and
- (3) Collaborate with the agency ISSPM or Administrators of Domain Servers to ensure that a complete inventory is maintained for all agency Web sites, including Point of Contact information.

-END-