U.S. DEPARTMENT OF AGRICULTURE
WASHINGTON, DC 20250

# DEPARTMENTAL REGULATION	**Number:** DR 3515-001
SUBJECT: Use of Web Measurement and Customization Technologies	**DATE:** October 21, 2011
	OPI: Office of the Chief Information Officer

1. PURPOSE

a. This Departmental Regulation (DR) establishes guidance for the use of web measurement and customization technologies and the associated privacy requirements for public-facing and third-party websites and applications owned or operated on behalf of the United States Department of Agriculture (USDA).

b. This directive does not apply to internal agency activities (such as intranets, applications, or interactions not involving the public) or to activities that are part of authorized law enforcement, national security, or intelligence activities.

c. This policy adheres to the guidance identified in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3 identified in the table below.

Identifier	Family	Class
AC-8	Access Control	Technical
PL-5	Planning	Management
PS-7	Personnel Security	Operational
SC-14	System and Communications Protection	Technical

2. SCOPE

Unless otherwise specified, this directive applies to all USDA agency and staff office personnel, including non-Government personnel (e.g., contractors, interns, and partners) authorized to use USDA web and application resources, including third-party websites, for official USDA purposes.

3. SPECIAL INSTRUCTIONS/CANCELLATIONS

This policy supersedes Departmental Manual (DM) 3515-001, *Collection of Web Page Cookies & Privacy Requirements*, dated August 19, 2004. The title of this policy has been changed to reflect changes in the terminology used by the Office of Management and Budget (OMB).

OMB Memorandum M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies* rescinds OMB Memorandum M-00-13, *Privacy Policies and Data Collection on Federal Websites* and the following specified sections in OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*: Section III(D)(2)(v) concerning tracking and customization activities, and Section VII(B) regarding the reporting of tracking technologies.

4. 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's information activities involving personal information. The Federal Government has established guidelines for the use of web measurement and customization technologies and to enable the useful functioning of federal websites while protecting individual privacy.

5. POLICY

a. Appropriate Use and Prohibitions

(1) Agencies may use web measurement and customization technologies (e.g., persistent cookies, web analytics, etc.) for the purpose of improving Federal services online through conducting measurement and analysis of usage or through customization of the user's experience.

(2) Agencies may not use web measurement and customization technologies to:

(a) track user individual-level activity on the Internet outside of the website or application from which the technology originates;

(b) share the data obtained through such technologies, without the user's explicit consent, with other departments or agencies;

(c) cross-reference, without the user's explicit consent, any data gathered from web measurement and customization technologies against PII to determine individual-level online activity;

(d) collect PII without the user's explicit consent in any fashion; or

(e) for any like usages so designated by OMB.

b. General Guidance

(1) Agencies will only collect or create information necessary for the proper performance of the agency's 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.

(2) Agencies must exercise care to ensure that they comply with OMB's privacy policies cited in Appendix B of this document and the requirements outlined in the Privacy Act of 1974. The Privacy Act allows individuals to access documents maintained in a Privacy Act system of records and to request amendments to the records.

(3) Visitors to a USDA website must receive clear and conspicuous notification in the Department's privacy notice regarding the use of technologies for collecting an individual's information and how that information will be used.

(4) Agencies will comply with the standards set forth in the Children's Online Privacy Protection Act of 1998 (COPPA) with respect to the collection of personal information directed at children. USDA will not knowingly contact or collect personal information or solicit information of any kind for children under the age of 13.

It is possible that by fraud or deception we may receive information pertaining to children under the age of 13. If such actions are detected, the USDA Chief Privacy Officer should be notified via the Personally Identifiable Information (PII) Hotline and the information reviewed for further action.

c. Usage Tiers

OMB M-10-22 defines tiers for authorized use of web measurement and customization technologies.

(1) Tier 1 – single session. This tier encompasses any use of single session web measurement and customization technologies.

(2) Tier 2 – multi-session without PII. This tier encompasses any use of multi-session web measurement and customization technologies when no PII is collected (including when the agency is unable to identify an individual as a result of its use of such technologies).

(3) Tier 3 – multi-session with PII. This tier encompasses any use of multi-session web measurement and customization technologies when PII is collected (including when the agency is able to identify an individual as a result of its use of such technologies).

More detailed information pertaining to usage tiers and associated privacy requirements can be found in OMB M-10-22, Attachments 1 and 2.

d. Third-Party Website Usage

(1) Before an agency uses a third-party website or application to engage with the public, the agency must follow the process identified in DR 1495-001, *New Media Roles, Responsibilities, and Authorities,* which requires evaluation by the Office of Communications (OC) and Office of the Chief Information Officer (OCIO) prior to use and implementation of the third-party site. The agency shall, at a minimum, review the third-party's privacy policy quarterly to confirm appropriateness and reassess risk.

(2) Before an agency uses a third-party website or application to engage with the public, the agency must exercise due diligence to determine whether the third-party's website or application contains links to sites that may provide content not supported or endorsed by the Department. The agency shall, at a minimum, review the third-party's website quarterly to confirm appropriateness.

(3) If an agency posts a link that leads to a third-party website or any other location that is not part of an official government domain, a statement adjacent to the link or visual alert must be provided to notify the user that they are being directed to a non-government website that may have different privacy policies from those of the agency's official website. Visual alerts must comply with federal regulations and policies.

(4) USDA agencies using a third-party website or application for content placement that is not part of an official government domain must ensure that appropriate USDA branding is applied to distinguish the agency's activities from those of non-government entities.

(5) Agencies utilizing a third-party service to solicit feedback must also provide an alternative government e-mail address where users can also send feedback.

(6) Information collected through an agency's use of a third-party website or application must only collect the information "…necessary for the proper performance of agency functions and which has practical utility."[1] If PII is collected, the agency shall collect only the minimum necessary to accomplish a purpose required by statute, regulation, or executive order.

e. Privacy Impact Assessments (PIA) and PII

(1) Agencies are required to perform a PIA whenever the use of a third-party website or application makes PII available to the agency.

(2) The PIA shall describe:

(a) The specific purpose of the agency's use of the third-party website or application;

(b) Any PII that is likely to become available to the agency through public use of the third-party website or application;

(c) The agency's intended or expected use of PII;

(d) With whom the agency will share PII;

(e) Whether and how the agency will maintain PII, and for how long;

(f) How the agency will secure PII that it uses or maintains;

(g) What other privacy risks exist and how the agency will mitigate those risks; and

(h) Whether the agency's activities will create or modify a "system of records" under the Privacy Act.

(3) In general, an agency's use of a third-party website or application shall be covered in a single, separate PIA. However, an agency may prepare one PIA to cover multiple websites or applications that are functionally comparable, as long as the agency's practices are substantially similar across each website and application.

[1] OMB Circular A-130, http://www.whitehouse.gov/omb/circulars_a130_a130trans4/

(4) If an agency's use of a website or application raises distinct privacy risks, the agency shall prepare a PIA that is exclusive to that website or application.

(5) If the agency's use of a website or application results in the ability to retrieve PII, the agency shall comply with the system of records notice requirement of the Privacy Act.

6. POLICY EXCEPTION REQUIREMENTS

All USDA agencies and staff offices are required to conform to the policy; however, in the event that a policy requirement cannot be met as explicitly stated, agencies may submit a waiver request. The waiver request must explain the reason for the request, identify compensating controls/actions that meet the intent of the policy, and identify how the compensating control/action provides a similar or greater level of defense or compliance than the policy requirement. Agencies and staff offices will submit all policy waiver requests directly to the Associate Chief Information Officer (ACIO) for Cyber Policy and Oversight (CPO) for review and decision.

Unless otherwise specified, agencies must review and renew approved policy waivers every fiscal year. Approved waivers must be recorded and tracked as a Plan of Action and Milestones (POA&M) item in the Department's Federal Information Security Management Act (FISMA) data management and reporting tool. CPO will monitor all approved waivers.

7. PROCEDURES AND GUIDANCE

This DR may be further shaped by other USDA regulations and manuals that contain clarifying procedures. USDA Departmental regulations and manuals can be found at: http://www.ocio.usda.gov/directives/index.html. Additional references can also be found in Appendix B of this directive.

8. RESPONSIBILITIES

a. The USDA Chief Information Officer (CIO) and Director, Office of Communications will:

(1) Ensure that USDA agencies/mission areas comply with current Federal and OMB guidance with regard to the use of web measurement and customization technologies and protection of PII; and

(2) Ensure that information resulting from the annual web measurement and customization technology system/procedure reviews are posted on the agency's "USDA.gov/open" page and a public feedback mechanism established.

b. The Associate CIO for Cyber Policy and Oversight (ACIO-CPO) will:

(1) Publish minimum requirements identifying the Department's approach to OMB and other relevant Federal agency-issued web measurement and customization technologies and privacy guidance;

(2) Issue direction to cease operating websites if the agency/mission area or contractor is not in compliance with the policies identified in this directive and does not correct the problem in a timely manner (within 2 working days).

(3) Review and render decision on waivers to the guidance established in this policy.

c. The USDA Chief Privacy Officer and Agency Privacy Act Officers will:

(1) Ensure that USDA agencies/mission areas and contractors comply with the requirements of the Privacy Act and COPPA with regard to the collection and use of personal information.

(2) At a minimum, annually review the online privacy notice on the www.USDA.gov page to ensure the notice provides the public with the most current guidance and information.

d. The Office of the Inspector General (OIG) will:

Incorporate a review of applicable requirements concerning the use of web measurement and customization technologies and posting of privacy notices in their audit of USDA websites, as appropriate.

e. The Office of the General Counsel (OGC) will:

(1) Review applicable legal documentation in the form of new media site Terms of Service (TOS) agreements;

(2) Providing the Department and agencies with legal guidance and advice on issue-specific situations; and

(3) Providing enforcement justifications for the removal or deactivation of Department or agency profiles and accounts based upon agency or department staff performance or utilization, content, or other issue with legal implications for the Department or agency.

f. The Agency/Mission Area CIOs will:

(1) Implement this policy within their respective agency and/or office;

(2) Ensure that all agency internet and intranet websites are inventoried and the inventory list provided to the ACIO CPO and/or Director, Office of Communications, upon request;

(3) 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; and

(4) Promptly notify the ACIO-CPO of any web sites that do not comply with privacy requirements.

g. The Agency/Mission Area Information Systems Security Program Managers (ISSPM) will:

Conduct periodic reviews of websites as part of overall security compliance to ensure that USDA agencies/contractors are appropriately utilizing persistent cookies, web agents, and other web technologies appropriately and ensure sites are providing the public with conspicuous access to the USDA privacy notice.

h. The Agency System Administrator(s)/Webmaster(s) will:

(1) Prepare and maintain a complete inventory list of all agency internet and intranet websites, update this list monthly or as changes occur, and provide a copy of the inventory list to the agency ISSPM. This list must include point of contact information (name, phone number, location, e-mail address) for each website;

(2) Ensure that all agency websites provide clear and conspicuous notice of USDA's privacy notice concerning individuals and children upon entering all sites, in compliance with the requirements of this policy; and

(3) Monitor and verify that all agency websites comply with the requirements of the Privacy Act and COPPA with regard to the collection and use of personal information.

-END-

APPENDIX A

DEFINITIONS

Individual: A citizen of the United States or an alien lawfully admitted for permanent residence.

Persistent Cookies: A small text file containing a collection of information, usually a user name and the current date and time, that is stored on a computer and used to identify a user who has previously registered or visited a website. A persistent cookie, also called a permanent cookie or stored cookie, operates until it expires or until a user deletes it.

Privacy Impact Assessment (PIA): An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Personally Identifiable Information (PII): PII refers to information that can be used to distinguish or trace an individual's identity. Examples include a person's name, social security number, or other information that alone or when combined with other identifying information, is linked or linkable to a specific individual.

Privacy notice: A statement made by an organization regarding why, how, and pursuant to what legal authority (if applicable) personal data is being collected at a public website or social media site, and how the owner of the site will use any information obtained.

Privacy policy: In relation to OMB M-10-23 and this directive, the term "privacy policy" refers to a single, centrally located statement that is accessible from an agency's official homepage. The privacy policy should be a consolidated explanation of the agency's general privacy-related practices that pertain to its official website and its other online activities

Record: A record under the Privacy Act means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print (biometrics), or a photograph.

System of records: A Privacy Act system of records is a group of any records (as defined by the Privacy Act) under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

Third-party websites or applications: The term "third-party websites or applications" refers to web-based technologies that are not exclusively operated or controlled by a government entity, or web-based technologies that involve significant participation of a non-government entity. Often these technologies are located on a ".com" website or other location that is not part of an official government domain. However, third-party applications can also be embedded or incorporated on an agency's official website.

Web measurement and customization technologies: Technologies used to remember a user's online interactions with a website or online application in order to conduct measurement and analysis of usage or to customize the user's experience.

APPENDIX B

AUTHORITIES AND REFERENCES

Children's Online Privacy Protection Act of 1998 (COPPA) (15 U.S.C. 6501, et seq.)

Departmental Regulation (DR) 4070-735-001, "Employee Responsibilities and Conduct," October 4, 2007

DR 1495-001, "New Media Roles, Responsibilities and Authorities," May 23, 2011

DM 3515-002, "Privacy Impact Assessment," February 17, 2005

NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations"* (Errata as of May 1, 2010)

NIST SP 800-95, *Guide to Secure Web Services,* August 2007

NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* April 2010

OMB Memorandum M-99-18, *"Privacy Policies on Federal Websites",* June 2, 1999

OMB Memorandum M-10-22, *"Guidance for Online Use of Web Measurement and Customization Technologies"*, June 25, 2010

OMB Memorandum M-10-23, *"Guidance for Agency Use of Third-Party Websites and Applications",* June 25, 2010

OMB Memorandum M-03-22, "*Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002",* September 26, 2003 (modifies M-00-13, June 22, 2002)

The Privacy Act of 1974 (5 U.S.C. 552a, et seq.)

USDA Web Standards and Style Guide v1.1, April 18, 2011

APPENDIX C

ABBREVIATIONS

ACIO	Associate Chief Information Officer
CIO	Chief Information Officer
COPPA	Children's Online Privacy Protection Act of 1998
CPO	Cyber Policy and Oversight
DM	Departmental Manual
DR	Departmental Regulation
ISSPM	Information Systems Security Program Manager
NIST	National Institute of Standards and Technology
OC	Office of Communications
OCIO	Office of the Chief Information Officer
OGC	Office of the General Counsel
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
SP	Special Publication
USDA	United States Department of Agriculture