

NATIONAL WEATHER SERVICE POLICY DIRECTIVE 60-6

March 22, 2016

Information Technology

Information Technology Privacy Policy

NOTICE: This publication is available at: <http://www.nws.noaa.gov/directives/>.

OPR: ACIO (S. Richardson)

Certified by: ACIO (R.Varn)

Type of Issuance: Routine

SUMMARY OF REVISIONS: This directive supersedes NWS Policy Directive 60-6, Information Technology Privacy Policy, and dated October 24, 2014. Changes made to reflect the NWS Headquarters reorganizations effective April 1, 2015

Changes: OPR by, Certified by, 3.2, CIO to ACIO; removed 3.2 b, c, d; changed 3.3 context; removed reference of national and local policy; changed 3.4 from Program manager to ISSO; deleted a. and changed b, c, d content to be in line with DOC IT Privacy policy.

1. Information Technology (IT) Privacy is the protection of confidentiality of personal or business information that is identified to the individual or business. This information is collected from respondents through information collection activities or from other sources and is maintained by the Department of Commerce (DOC) in IT systems. This information is called “identifiable information.” Office of Management and Budget (OMB) guidance, consistent with the E-Government Act of 2002, protects personally identifiable information. NWS, through this policy, is extending the same protection to business identifiable information.
2. The objective of the IT Privacy Policy is to ensure NWS systems maintain an adequate level of IT privacy for any information collected using IT resources under NWS control.
3. This directive established the following authorities and responsibilities:
 - 3.1 The Assistant Administrator for National Weather Services (AA/NWS) is responsible for overseeing adequate protection of confidentiality of personal or business information of an individual or business.
 - 3.2 The Associate Chief Information Officer (ACIO) for Weather is responsible for ensuring IT privacy policy and guidance are developed and ensures their dissemination and implementation throughout NWS. This includes policy and guidance for Web Privacy, Privacy Impact Assessments (PIA), and posting of privacy policies on NWS websites used by the public.
 - 3.3 The NWS Information Technology Security Officer (ITSO) will review PIAs, and Privacy Threshold Analysis (PTA), before submission to the NOAA Privacy Officer Designee for final approval.

3.4 The System Owner is responsible for providing an adequate and appropriate level of protection of confidentiality for individual or business personal identifiable information that is collected using IT resources under their control. System level IT privacy will ensure information confidentiality and integrity are commensurate with NWS business needs for information collection in the accomplishment of the organization's mission. The system owner will:

- a. Collect only the minimal amount of information necessary from individuals and businesses required by the Agency's mission and legal requirements.
- b. Provide a notice, stated in a clear manner, describing the purpose of the collection and use of the identifiable information. Information collected will not be used for any other purpose unless authorized or mandated by law.
- c. Ensure that information collected is maintained in a sufficiently confidential, accurate, timely, and complete manner to ensure that the interest of the individuals and business are protected.
- d. Implement adequate physical and IT security measures as prescribed to ensure that the collection, use, and maintenance of identifiable information is properly safeguarded and the information is promptly destroyed in accordance with approved records control schedules.

3.5 The Information System Security Officer will:

- a. Incorporate this policy as required.
- b. For new systems or major modifications determine whether there is a need for a PIA, based on DOC IT Privacy Policy definitions.
- c. Conduct the PIA and submit to the NW ITSO for review and NOAA Privacy Officer Designee for approval.
- d. Conduct an annual Privacy Threat Analysis (PTA) for each system under their authority as part of the annual re-authorization.

4.0. This policy directive is supported by the references listed in Attachment 1.

Signed

3/08/2016

Louis W. Uccellini
Assistant Administrator for Weather Services

Date

Attachment 1

References and Supporting Information

1. The Privacy Act of 1974 (**5 USC 552a**) regulates the Federal Government's collection, use, maintenance, and dissemination of information about individuals.
2. Section 208 of the E-Government Act of 2002 (**44 USC 3601 et seq**) establishes procedures to ensure the privacy of personal information in electronic records (specific citation for Section 208 is **44 USC 3501** note).
3. The Paperwork Reduction Act (PRA) of 1995 (**44 USC 3501 et seq.**) is designed to reduce the public's burden of answering unnecessary, duplicative, and burdensome government surveys.
4. The Trade Secrets Act (**18 USC 1905**) provides criminal penalties for the theft of trade secrets and other business identifiable information.
5. The Children's Online Privacy Protection Act of 1998 (**15 USC 6501-06**) regulates the online collection and use of personal information provided by and relating to children under the age of 13.
6. OMB Circular A-130, "Management of Federal Information Resources," establishes a policy for the management of Federal information resources, including automated information systems.
7. OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 26, 2003, provides specific guidance to agencies for implementing Section 208 of the E-Government Act.
8. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, establishes requirements to review and reduce the volume of PII; eliminate the unnecessary use of social security numbers (SSN); and log all computer-readable data extracts from databases holding sensitive information and verify each extract, including whether sensitive data has been erased within 90 days or its use is still required (pages 6-8).
9. OMB Memorandum M-06-16, Protection of Agency Sensitive Information, provides guidance for encrypting sensitive data on mobile computers and devices; allowing remote access only with two-factor authentication; using a time-out function for remote access; and logging all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required.
10. OMB Memorandum M-06-15, Safeguarding Personally Identifiable Information, requires that agencies conduct a review of their policies and processes, and take corrective action as appropriate to ensure adequate safeguards to prevent the intentional or negligent misuse of, or unauthorized access to, personally identifiable information.
11. Department of Commerce IT Privacy Policy provides a guidance, definitions, and background regarding PIAs.
12. NOAA OCIO website for PIA: http://www.cio.noaa.gov/services_programs/pia.html
13. NWSPD 60-1, Technical and Content Requirements for Internet Servers, addresses the webprivacy policy and posting requirement (OUTDATED POLICY)