NATIONAL WEATHER SERVICE POLICY DIRECTIVE 60-6
JUNE 28, 2022

Information Technology

DIGITAL PRIVACY POLICY

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

OPR: W/ACIO (Paula Reis-Cypress) **Certified by:** W/ACIO (Beckie Koonge)
Type of Issuance: Routine

SUMMARY OF REVISIONS: This directive supersedes NWS Policy Directive 60-6, Information Technology Privacy Policy, dated March 22, 2016. This is a routine review and update to keep this document current, increase applicability, and reduce ambiguity. Editorial changes were made to ensure clear and concise policy guidance and improve readability.

1. Digital Privacy is the protection of personally identifiable information (PII) or business identifiable information (BII) that is collected from respondents through information collection activities or from other sources and that is maintained by the DOC in its information technology (IT) systems. For purposes of this policy, this information is termed "identifiable information." Office of Management and Budget (OMB) guidance, consistent with the E-Government Act of 2002, protects PII. NWS, through this policy, is extending the same protection to BII.

2. The objective of the Digital Privacy Policy is to ensure NWS systems maintain an adequate level of digital privacy for any identifiable 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 managing NWS personnel and polices to provide adequate protection of identifiable information for individuals or businesses.

3.2 The Assistant Chief Information Officer (ACIO) for Weather is responsible for ensuring IT privacy policy and guidance are developed, disseminated, and implemented throughout NWS. This includes policy and guidance for Web Privacy, Privacy Impact Assessments (PIA), and posting of privacy policies on NWS websites utilized by the public.

3.3 The NWS Information Technology Security Officer (ITSO) will review Privacy Threshold Analyses (PTAs), and Privacy Impact Assessments (PIAs), before submission to the NOAA Privacy Office for final review and approval.

3.4 The System Owner (SO) is responsible for providing an adequate and appropriate level of confidentiality and integrity protection for identifiable information that is collected using IT resources under their purview, and ensures that it is commensurate with NWS business needs for information collection in the accomplishment of the organization's mission. The SO will:

a. Collect the minimal amount of information necessary from individuals and businesses consistent with the Agency's mission and legal requirements.

b. Provide a notice written in a clear manner covering the purposes of the collection and use of 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 interests of the individuals and businesses are protected.

d. Implement adequate physical and IT security measures 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 (ISSO) will:

a. Incorporate this policy as required.

b. For new systems or major modifications of an existing system, determine whether there is a need for a PIA, based on Department of Commerce IT Privacy Policy requirements.

c. Conduct an annual PTA for each system under their authority as part of the annual re-authorization.

d. If required by the PTA, conduct an annual PIA as part of the annual re-authorization and submit to the NWS ITSO for review and NOAA Privacy Office for review and approval.

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

GRAHAM.KENNETH.EARL.1365881142

Digitally signed by GRAHAM.KENNETH.EARL.1365881142
Date: 2022.06.14 15:56:05 -05'00'

Kenneth E. Graham
Assistant Administrator for
Weather Services

Date

Appendix 1

References and Supporting Information

1. The Privacy Act of 1974 (5 USC 552a) provides privacy protections for records containing information about individuals (i.e., citizen and legal permanent resident) that are collected and maintained by the federal government and are retrieved by a personal identifier. The Act requires agencies to safeguard information contained in a system of records (SOR).
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) (COPPA) regulates the online collection and use of personal information provided by and relating to children under the age of 13.
6. OMB Circular A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act, which describes agency responsibilities for implementing the review, reporting, and publication requirements of the Privacy Act of 1974 ("the Privacy Act"), and related OMB policies.
7. OMB Circular A-130, Management of Federal Information Resources, provides uniform government-wide information resources management policies as required by the Paperwork Reduction Act of 1980, as amended by the Paperwork Reduction Act of 1995, 44 U.S.C. Chapter 35.
8. OMB Memorandum M-03-22, Guidance for Implementing the Privacy Provisions of the E- Government Act of 2002, (September 26, 2003), requires agencies to conduct reviews of how information about individuals is handled when information technology (IT) is used to collect new information, or when agencies develop or buy new IT systems to handle collections of personally identifiable information (PII), and describes how the agency handles information that individuals provide electronically.
9. OMB Memorandum M-17-12, Preparing for and responding to a Breach of Personally Identifiable Information, sets forth the policy for Federal agencies to prepare for and respond to a breach of personally identifiable information (PII).
10. DOC Privacy Program Plan provides an overview of the Department's privacy program.
11. DOC Guide to Effective Privacy Impact Assessments (PIA) provides a framework for conducting PIAs at the DOC and a methodology for assessing how PII is to be managed in electronic information systems.

12. NOAA OCIO website for Privacy: https://www.noaa.gov/organization/information-technology/privacy
13. NWSPD 60-1, Technical and Content Requirements for Internet Servers, addresses the web privacy policy and posting requirement.
14. Executive Order No. 13556 - Controlled Unclassified Information, Vol. 75, No. 216 (November 4, 2010) establishes a program for managing all unclassified information in the Executive branch that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies.