NIST SP 800 – 53r4
APPENDIX J CONTROL ALLOCATIONS and IMPLEMENTATION STATEMENTS

Control Types

a. **Common:** Single implementation leveraged and used uniformly across the Department.
b. **Hybrid:** Implementation is split between two or more elements of the Department.
c. **System:** Implementation is unique to the specific system.

ID	Privacy Controls	Identified Control
AP	**Authority and Purpose**	Control Type
AP-1	Authority to Collect: The organization determines and documents the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), either generally or in support of a specific program or information system need.	**NOAA Level – Hybrid** **NOAA Level:** Determine from review of the PIA, review of applicable system of records notice(s) (SORN(s)) and any Privacy Act (PA) Statements. **System Level:** Documented in the system's PIA introduction, the applicable (SORN(s))(PIA Section 9) and any PA statements (PIA Section 7.1).
AP-2	Purpose Specification: The organization describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices.	**NOAA Level – Hybrid** **NOAA Level:** Determine from review of the PIA and applicable SORN(s). **System Level:** Documented in the system's PIA, Section 5.1.
AR		
AR-1	Governance and Privacy Program **– *NA for system level assessment.***	**COMMON –** **DEPT Level – DOO 10-19; DOO 20-31**
AR-2	Privacy Impact and Risk Assessment: a. Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII) b. b. Conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.	**NOAA Level – Hybrid** **NOAA Level:** BPO risk assessment process equates to *review* of SORN, PTA/PIA, and PA Statements developed at the system level. **System Level:** *Develop* annual PTA and develop/revise PIA when needed, select applicable SORN(s), develop PA Statements.

NIST SP 800 – 53r4
APPENDIX J CONTROL ALLOCATIONS and IMPLEMENTATION STATEMENTS

AR-3	Privacy Requirements for Contractors and Service Providers: a. Establishes privacy roles, responsibilities, and access requirements for contractors and service providers. b. Includes privacy requirements in contracts and other acquisition-related documents.	**HYBRID –** **DEPT Level** – CAM 1337.7; DOC Privacy Plan (TBD) **NOAA Level – Hybrid** **NOAA Level:** Reviews PIA and enquires regarding applicable FAR section in contracts. **System Level:** Documents in PIA Section 8.1 and ensures applicable FAR section are in contracts.
AR-4 POA&M 70893	Privacy Monitoring and Auditing: Monitors and audits privacy controls and internal privacy policy to ensure effective implementation.	**HYBRID –** **DEPT Level** – DOC Data Loss Prevention (DLP) Policy – bureaus have DLP tool(s) implementation plan by 9-30-15 and in place by Q1, FY17. Annual review of privacy controls. **NOAA Level – Hybrid** **NOAA Level:** DLP Plan approved at NOAA level and submitted to DOC. Privacy Monitoring Tools/Capabilities: A&A Authorization for FIPSs 199 high impact systems. Continuous review of privacy controls. **System Level:** Prepare for A&As, authorization at LO level for FIPSs 199 moderate and high impact systems. Continuous review of privacy controls.
AR-5 POA&M 70897	Privacy Awareness and Training: a. Develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures b. Administers basic privacy training annual and to new hires and annual targeted, role-based privacy training for personnel having responsibility for personally identifiable information (PII) or for activities that involve PII c. Ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements.	**HYBRID –** **DEPT Level** – DOC Privacy Training/ Awareness **NOAA Level – Hybrid** **NOAA Level:** Annual privacy awareness training and role-based training (role-based training in development). **System Level:** Ensure that those whose roles include responsibility for PII or activities that involve PIA: 1. Take the (probably Web-based) training annually and 2. Certify acceptance of privacy requirements responsibility.

AR-6	Privacy Reporting: The organization develops, disseminates, and updates reports to the Office of Management and Budget (OMB), Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance. ***NA for system level assessment.***	**COMMON –** **DEPT and NOAA Level** –DOC and NOAA Breach Response Plans, and DEPT and NOAA Annual FISMA/ Privacy Reports
AR-7 POA&M 70901	Privacy-Enhanced System Design and Development: Designs information systems to support privacy by automating privacy controls.	**NOAA Level –Hybrid** **NOAA Level:** Determination of standard tools. **System Level:** Implementation.
AR-8	Accounting of Disclosures: a. Keeps an accurate accounting of disclosures of information held in each system of records under its control, including: (1) Date, nature, and purpose of each disclosure of a record; and (2) Name and address of the person or agency to which the disclosure was made b. b. Retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer; and c. Makes the accounting of disclosures available to the person named in the record upon request. (for routine sharing with another agency, individual accounting may not be required).	**NOAA Level –Hybrid** **NOAA Level:** Review of the PIA and enquiry re disclosure log. **System Level:** Documented in the PIA, Introduction and Section 6.1
DI	**Data Quality and Integrity**	

NIST SP 800 – 53r4
APPENDIX J CONTROL ALLOCATIONS and IMPLEMENTATION STATEMENTS

DI-1	Data Quality a. Confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information b. Collects PII directly from the individual to the greatest extent practicable c. Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems [*annually*] d. Issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.	**NOAA Level –Hybrid** **NOAA Level:** Review of the PIA and SORN. Use NOAA Information Quality Guidelines as a reference regarding quality, utility, objectivity, and integrity of disseminated information. **System Level:** During NOAA review, clearly provide or amplify on purpose for collection of specific data elements, when requested (information in Section 5.1). Collect PII directly from individual to the greatest extent possible e.g. via applications or through accounts created by members of the public requesting information.
DI-2	Data Integrity and Data Integrity Board a. Documents processes to ensure the integrity of personally identifiable information (PII) through existing security controls b. Establishes a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements and to ensure that those agreements comply with the computer matching provisions of the Privacy Act.	**NOAA Level –Hybrid** **NOAA Level**: Assessment of applicable security controls in conjunction with PIA review. (b. is NA at this point since no computer matching agreements). **System Level:** Ensures that applicable security controls are in place or have a POA&M (Sections 8.1 and 8.2).
DM	**Data Minimization and Retention**	
DM-1	Minimization of Personally Identifiable Information a. Identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection b. Limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent c. Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings, at least annually, to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.	**NOAA Level –Hybrid** **NOAA Level:** Review of PIA to determine that only PII needed for the stated purpose is collected. Overlaps with DI-1(b) **System Level:** a. Clearly documented in the PIA, Sections 4.1 and 5.1, the purpose for each type of PII and BII. b. Conducts an initial evaluation, when developing or revising a PIA, and annually thereafter, to determine only PII needed for the stated purpose is collected.

DM-2	Data Retention and Disposal a. Retains each collection of personally identifiable information (PII) for the time specified in the applicable record schedule[to fulfill the purpose(s) identified in the notice or as required by law; b. Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule (the above applicable schedule) and in a manner that prevents loss, theft, misuse, or unauthorized access c. Uses techniques or procedures defined by the applicable records schedule to ensure secure deletion or destruction of PII (including originals, copies, and archived records).	**NOAA Level –Hybrid** **NOAA Level:** Reviews the listed records schedules in the PIA, to ensure applicable and complete. **System Level** –Documents in the PIA, Section 10, the applicable records schedules.
DM-3	Minimization of PII Used in Testing, Training, and Research a. Develops policies and procedures that minimize the use of personally identifiable information (PII) for testing, training, and research; and b. Implements controls to protect PII used for testing, training, and research.	**HYBRID –** **DEPT Level** – DOC Privacy Plan (TBD) **NOAA Level –Hybrid –** **NOAA Level –** If use of PII in testing and training is documented, discourages use /or if used, require explanation. **System Level** – If PII is used in testing and training (documented in PIA, Sections 2.1 and 5.1), clearly justify, or eliminate use, which may including consulting a GC. If justified, ensure applicable controls are in place.
IP	**Individual Participation and Redress**	

NIST SP 800 – 53r4
APPENDIX J CONTROL ALLOCATIONS and IMPLEMENTATION STATEMENTS

IP-1	Consent a. Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection b. Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII c. Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII d. Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.	**NOAA Level –Hybrid** **NOAA Level** – Reviews PIA, any PA statements, and applicable SORNs. **System Level** - Documents, for each group from which PII is collected, in the PIA, Section 7.2 and 7.3 and develops and includes in forms/posts on Web sites, PA statements which address statutory authority, purpose, routine uses and disclosure.
IP-2	Individual Access a. Provides individuals the ability to have access to their personally identifiable information (PII) maintained in its system(s) of records b. Publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records c. Publishes access procedures in System of Records Notices (SORNs) d. Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.	**HYBRID –** **DEPT Level** – SORN and PIA **NOAA Level** – Hybrid– Review of SORN, which will cover general access and PIA, for specific access. **Privacy Act Officer** – When developing or coordinating on a SORN, ensure access procedures are included. Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests. System Level – Ensures that the individual access process is documented in the PIA, Section 7.4.

IP-3	Redress a. Provides a process for individuals to have inaccurate personally identifiable information (PII) maintained by the organization corrected or amended, as appropriate. b. Requires the organization to inform the individual of its refusal to amend in accordance with the request, the reason for refusal, and the procedures for administrative appeal. c. Requires the organization to establish an process through which individuals can appeal the decision to refuse to amend their information pursuant to 552a(d)(3).	**HYBRID –** **DEPT Level** – DOC Privacy Act Handbook **NOAA Level –Hybrid** **NOAA Level** – Review of SORN, PIA, and PA Statements. **System Level** – Documents in PIA, Section 7.4.
IP-4	Complaint Management The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices. ***NA for system level***	**HYBRID –** **DEPT Level** – DOC Privacy Act Handbook **NOAA Level** - Common – Privacy Policy link on all Web sites has feedback option.
SE	**Security**	

SE-1	Inventory of Personally Identifiable Information a. Establishes, maintains, and updates [*Assignment: organization-defined frequency*] an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII) b. Provides each update of the PII inventory to the CIO or information security official [*Assignment: organization-defined frequency*] to support the establishment of information security requirements for all new or modified information systems containing PII. ***NA for system level***	**HYBRID –** **DEPT Level** – SAOP FISMA Guidance and Reporting **NOAA Level –Common** – SORNs and PIAs feed NOAA inventory, but no actual data mining in place. – NOAA Privacy Office responds to an annual SAOP data call, describing types of PII collected for each system
SE-2	Privacy Incident Response a. Develops and implements a Privacy Incident Response Plan; and b. Provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan. ***NA for system level***	**HYBRID–** **DEPT Level** – DOC Breach Response Plan **NOAA Level –Common** - Response plan is addressed in NOAA Privacy Plan, CIRT, Breach Response Processes
TR	**Transparency**	

TR-1	Privacy Notice a. Provides effective notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII); (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary b. Describes: (i) the PII the organization collects and the purpose(s) for which it collects that information; (ii) how the organization uses PII internally; (iii) whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII; and (vi) how the PII will be protected c. Revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change.	**NOAA Level –Hybrid** – See also IP-1 **NOAA Level** – Review of SORN, PIA and PIA statement. Public notices regarding changes in practice or policy affecting PII. **System Level –** Documents in PIA, Section 7 and related PA statements. Provides public notice (in PIA) regarding changes in its activities that impact privacy, before or as soon as practicable after the change.

ID	Privacy Controls	Identified Control
TR-2	System of Records Notices and Privacy Act Statements a. Publishes System of Records Notices (SORNs) in the Federal Register, subject to required oversight processes, for systems containing personally identifiable information (PII) b. Keeps SORNs current c. Includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.	**NOAA Level –Hybrid** **NOAA Level** - Works with systems to keep SORNs current and submit to DOC for review. Reviews SORN, PIA and PA Statements. **System Level** – Works with NOAA to keep SORNs current. Develops PA statements as applicable and includes urls in the PIA, Section 7.1 or includes copies in the PIA submitted for DOC review.

TR-3	Dissemination of Privacy Program Information a. Ensures that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) b. Ensures that its privacy practices are publicly available through organizational websites or otherwise. ***NA for system level***	**COMMON –** **DEPT Level** – DOC Privacy Plan (TBD), and DOC Privacy Website **NOAA Level –Common –** NOAA Privacy Plan and NOAA Privacy Web site – both public-facing
UL	**Use Limitation**	
UL-1	Internal Use The organization uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.	**NOAA Level –Hybrid** **NOAA Level** - Monitoring and auditing organizational use and training; review of SORN and PIA. **System Level**, authorized use compatible with Privacy Act, PIA Section 2.1
UL-2	Information Sharing with Third Parties a. .Shares personally identifiable information (PII) externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes b. Where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used c. Monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII d. Evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.	**NOAA Level –Hybrid** **NOAA Level** - Monitoring of MOAs; system-level, document use under authorized purposes, compatible with Privacy Act, review PIA. Provides role-based training for those handling PII. **System Level –** Document in PIA Section 6.1, reference MOAs if applicable.

NIST SP 800 – 53r4
APPENDIX J CONTROL ALLOCATIONS and IMPLEMENTATION STATEMENTS