

NIST SP 800 – 53r4
APPENDIX J CONTROL ALLOCATIONS

Control Types

- a. **Common:** Single implementation leveraged and used uniformly across the Department (or if indicated, across NOAA).
- b. **Hybrid:** Implementation is split between two or more elements of the Department, or for NOAA, between NOAA-level and system-level. *If you see only NOAA-Level for a control, that means DOC has left it up to the bureau to allocate the control.*
- 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	NOAA Level – Hybrid In place, as PIAs and SORNs are updated, BCPO reviews –documented in privacy plan
AP-2	Purpose Specification	NOAA Level – Hybrid In place, as PIAs and SORNs are updated, BCPO reviews –documented in privacy plan
AR	Accountability, Audit, and Risk Management	
AR-1	Governance and Privacy Program	COMMON – DEPT Level – DOO 10-19; DOO 20-31
AR-2	Privacy Impact and Risk Assessment	NOAA Level – Hybrid System/Program Level – BCPO risk assessment process encompasses review of SORN, PTA/PIA, and PA Statements developed at the system level
AR-3	Privacy Requirements for Contractors and Service Providers	HYBRID – DEPT Level – CAM 1337.7; DOC Privacy Plan (TBD) NOAA Level – Hybrid – Contract Privacy Provision. OCIO ensures that it is carried out at program level --in place, but need to ensure documentation and consistency

NIST SP 800 – 53r4

APPENDIX J CONTROL ALLOCATIONS

AR-4	Privacy Monitoring and Auditing	<p>HYBRID – DEPT Level – DOC Data Loss Prevention (DLP) Policy – bureaus must have DLP tool(s) implementation plan by 9-30-15 and in place by Q1, FY17.</p> <p>NOAA Level – Hybrid – DLP planning in process by GPD and CSD. Privacy Monitoring Tools/ Capabilities: Systems prepare for A&As, authorization at LO level (moderate) or NOAA level (high) (DLP TBD, response in process to DOC data call 9/15)</p>
AR-5	Privacy Awareness and Training	<p>HYBRID – DEPT Level – DOC Privacy Training/Awareness NOAA Level – Hybrid – Bureau/ System Privacy Training/Awareness and Program level requirements - references AT-2, Security Awareness Training and AT-3, Role-Based Security Training. We are reviewing Census role-based training and may adapt for NOAA.</p>
AR-6	Privacy Reporting	<p>COMMON – DEPT and NOAA Level –DOC and NOAA Breach Response Plans, and DEPT and NOAA Annual FISMA/ Privacy Reports</p>
AR-7	Privacy-Enhanced System Design and Development	<p>NOAA Level –Hybrid Enterprise level determination of standard tools, implementation at system level. <i>Until tool(s) selected at the NOAA level, systems would be in compliance, as a default.</i></p>
AR-8	Accounting of Disclosures	<p>NOAA Level –Hybrid System/Program Level, as described in SORN and PIA and reviewed at NOAA Level (new question in 2015 PIA introduction)</p>
DI	Data Quality and Integrity	
DI-1	Data Quality	<p>NOAA Level –Hybrid Implemented at system level and reviewed as part of PIAs and SORNs</p>
DI-2	Data Integrity and Data Integrity Board	<p>NOAA Level –Hybrid System controls implemented/maintained and reviewed at NOAA Level as part of PIAs</p>
DM	Data Minimization and Retention	

NIST SP 800 – 53r4

APPENDIX J CONTROL ALLOCATIONS

DM-1	Minimization of Personally Identifiable Information	NOAA Level –Hybrid NOAA Level reviews PIA and determines that only PII needed for stated purpose is collected.
DM-2	Data Retention and Disposal	NOAA Level –Hybrid System/Program Level –PIA review including ensuring that applicable records schedules are listed.
DM-3	Minimization of PII Used in Testing, Training, and Research	HYBRID – DEPT Level – DOC Privacy Plan (TBD) NOAA Level –Hybrid – NOAA Privacy Plan, if testing and training documented, discourage use of PII, or if used, consult GC for justification
IP	Individual Participation and Redress	
IP-1	Consent	NOAA Level –Hybrid System/ Program Level – SORN, PIA, and PA Statement, also covered in related Paperwork Reduction Act collections
IP-2	Individual Access	HYBRID – DEPT Level – SORN and PIA NOAA Level – Hybrid – SORN (general access) and PIA – individuals whose information is in the system – process documented in PIA, Section 7.4.
IP-3	Redress	HYBRID – DEPT Level – DOC Privacy Act Handbook NOAA Level –Hybrid System/Program Level – SORN, PIA, and PA Statements – documented in PIA, Section 7.4
IP-4	Complaint Management	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	HYBRID – DEPT Level – SAOP FISMA Guidance and Reporting NOAA Level –Common – SORNs and PIAs feed NOAA inventory, but no actual data mining in place at this time.

NIST SP 800 – 53r4

APPENDIX J CONTROL ALLOCATIONS

SE-2	Privacy Incident Response	HYBRID– DEPT Level – DOC Breach Response Plan NOAA Level –Common - CIRT, Breach Response
TR	Transparency	
TR-1	Privacy Notice	NOAA Level –Hybrid – SORN, PIA (Section 7.1), and PA Statement. See also IP-1

NIST SP 800 – 53r4

APPENDIX J CONTROL ALLOCATIONS

ID	Privacy Controls	Identified Control
TR-2	System of Records Notices and Privacy Act Statements	NOAA Level –Hybrid NOAA level review of SORN, PIA and PA Statement developed at system level
TR-3	Dissemination of Privacy Program Information	COMMON – DEPT Level – DOC Privacy Plan (TBD), and DOC Privacy Website NOAA Level –Common – NOAA Plan and NOAA PIA Web site
UL	Use Limitation	
UL-1	Internal Use	NOAA Level –Hybrid NOAA-level; monitoring and auditing organizational use and training; system level, authorized use compatible with Privacy Act.
UL-2	Information Sharing with Third Parties	NOAA Level –Hybrid NOAA-level monitoring and signature of MOAs; system-level, document use under authorized purposes, compatible with Privacy Act.