Attachment D-6

Privacy Requirements:
Table of privacy laws, regulations, directives, policies, standards and guidelines

Authority	**Description**
Federal Records Act of 1950, 44 U.S.C. §§ 21, 29, 31 and 33	Establishes the framework used by Federal agencies for their Records Management programs.
The Freedom of Information Act (FOIA) of 1966, 5 U.S.C. § 552	This law provides the public with the right to request access to records from any Federal agency and requires that Federal information be made available to the public except under certain specified conditions.
The Privacy Act of 1974, 5 U.S.C. § 552a	This law imposes collection, maintenance, use, safeguard, and disposal requirements for Executive Branch offices maintaining information on individuals in a "system of records." This law also provides an individual a right to access and to amend any information about the individual in a system of records.
Federal Managers Financial Integrity Act of 1982 (FMFIA), 31 U.S.C. § 3512	This law mandates that Federal agencies establish and maintain an internal control program to safeguard data processing resources, assure their accuracy and reliability, and protect the integrity of information resident on such systems.
Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030	This law provides for the punishment of individuals who access Federal computer resources without authorization, attempt to exceed access privileges, abuse government resources, and/or conduct fraud on government computers.
Government Performance and Results Act (GPRA) of 1993, 31 U.S.C. § 1101	This law establishes policies for managing agency performance of mission, including performance of its practices.
Paperwork Reduction Act of 1995, Revised, 44 U.S.C. §§ 3501-3520	This law provides for the administration and management of computer resources.

Clinger-Cohen Act – Information Technology Management Reform Act of 1996, 40 U.S.C. § 1401, et seq.	This law improves the acquisition, use, and disposal of Information Technology (IT) by the Federal government.
Federal Financial Management Improvement Act (FFMIA) of 1996, 31 U.S.C. § 3111	This law mandates Federal agencies to implement and maintain financial management systems that comply substantially with Federal systems requirements, Federal accounting standards, and the U.S. Government Standard General Ledger (SGL). FFMIA also requires GAO to report annually on the implementation of the act.
National Information Infrastructure Protection Act of 1996, 18 U.S.C. § 1030	This law provides for the protection of computer resources.
Government Paperwork Elimination Act (GPEA) of 1998, 44 U.S.C. § 3504	This law provides for Federal agencies, by October 21, 2003, to give persons who are required to maintain, submit, or disclose information, the option of doing so electronically when practicable as a substitute for paper and to use electronic authentication methods to verify the identity of the sender and the integrity of electronic content.
E-Government Act of 2002, 44 U.S.C. § 101	This law enhances the management and promotion of electronic government services and processes by establishing a broad framework of measures requiring technology to enhance citizen access to government information services.
Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3541, as amended by the Federal Information Security Modernization Act of 2014, (Pub. L. 113-283)	FISMA requires Federal agencies to establish agency-wide risk-based information security programs that include periodic risk assessments, use of controls and techniques to comply with information security standards, training requirements, periodic testing and evaluation, reporting, and plans for remedial action, security incident response, and continuity of operations.

Applicable Programs include but are not limited to:

The Federal Risk and Authorization Program (FedRAMP)	FedRAMP is a Federally-centralized risk management program that enforces a standardized approach for assessing and monitoring the FISMA compliance of cloud products and services. The FedRAMP program requires cloud providers to receive an independent security assessment, conducted by a third-party assessment organization (3PAO), to sell government cloud services to a federal agency.

Applicable Executive Orders include but are not limited to:

Executive Order 10450, Security Requirements for Government Employees, April 1953	This order establishes that the interests of national security require all government employees be trustworthy, of good character, and loyal to the United States.
Executive Order 13011, Federal Information Technology, July 1996	This order establishes policy for the head of each agency to effectively use information technology to improve mission performance and service to the public.
Executive Order 13103, Computer Software Piracy, September 1998	This order establishes policy that each executive agency shall work diligently to prevent and combat software piracy in order to give effect to copyrights associated with computer software.
Presidential Decision Directive 63: Critical Infrastructure Protection, May 1998	This directive requires that the United States take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on critical infrastructures, including our cyber systems.
Executive Order 13231, Critical Infrastructure Protection in the Information Age, October 2001	This order establishes policy that ensures protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such information systems.

Executive branch policies established through directives published by OMB based on the applicable laws passed by Congress include:

OMB Circular	**Description**
A-11, Section 53, Information Technology and E-Government	This directive specifies the identification of security and privacy safeguards for managing sensitive information.
A-123, Management's Responsibility for Internal Control, as revised July 15, 2016	This directive specifies the policies and standards for establishing, assessing, correcting, and reporting on management controls in Federal agencies.
A-127, Financial Management Systems, as revised by Transmittal Memorandum Number 3, December 1, 2004	This directive prescribes policies and standards for executive departments and agencies to follow in developing, operating, evaluating, and reporting on financial management systems.
A-130, Appendix I, Responsibilities for Protecting and Managing Information Resources	This directive prescribes policy to agencies for the implementation of the Privacy Act and reporting requirements related to the management of personally identifiable information (PII).

Other requirements:

- OMB Memorandum M-05-24, *Implementation of Homeland Security Presidential (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors.*

- OMB Memoranda M-06-16, *Protection of Sensitive Agency Information*, , and M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, which establish requirements for the use of two-factor authentication for remote system access and requirements for responding to breaches or possible breaches of PII.

- OMB Memorandum M-08-05, *Implementation of Trusted Internet Connections*, which establishes the requirement for SSA to comply with the Trusted Internet Connection (TIC) initiative and the architectural requirements defined by the Department of Homeland Security (DHS) in the TIC Reference Architecture (current version 2.0 dated 2011).

- OMB Memorandum M-08-16, *Guidance for Trusted Internet Connection (TIC) Statement of Capability Form.*
- OMB Memorandum M-08-27, *Guidance for Trusted Internet Connection Compliance.*

- OMB Memorandum M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors.*

- OMB M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*.

- OMB M-14-04, *FY 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*.

- OMB M-16-17, *OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control*

- OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*

- OMB proposed guidance, *Improving Cybersecurity Protections in Federal Acquisitions*.

- National Security Presidential Directive and Homeland Security Presidential Directive (NSPD-54/HSPD-23), *Comprehensive National Cyber Security Initiative.*

- Homeland Security Presidential Directive (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*.

- Department of Homeland Security (DHS) Trusted Internet Connection (TIC), Version 2.0, Reference Architecture requirements.

- Federal Identity, Credential and Access Management (FICAM) Roadmap and Implementation Guidance and associated NIST standards regarding implementation and use of HSPD-12 Personal Identity Verification (PIV) two-factor SmartCard Public Key Infrastructure (PKI) based credentials for logical authentication.

- NIST Federal Information Processing Standard (FIPS) Publications.

- NIST 800-series Special Publications (SP).

- NIST Security Technical Implementation Guides (STIGs – also referred to as security configuration checklists).

- All management, operational and technical security control and continuous monitoring requirements as specified by FedRAMP.

- Federal Identity, Credential and Access Management (FICAM) Roadmap and Implementation Guidance.

- SSA TIC security architecture.