# Applicable laws and regulations

The following laws, regulations, or policies establish requirements for confidentiality, integrity, and availability for the Project Full Name. This document references the publications where appropriate.

## Federal statutes

* Federal Information Security Management Act of 2002 (FISMA)
  + <https://www.dni.gov/index.php/ic-legal-reference-book/federal-information-security-management-act>
* Federal Information Security Modernization Act of 2014 (FISMA 2014)
  + <https://www.dhs.gov/cisa/federal-information-security-modernization-act>
* OMB Circular A-130, Managing Federal Information as a Strategic Resource, July 2016
  + <https://www.cio.gov/policies-and-priorities/circular-a-130/>

## Federal standards and guidelines

* NIST Special Publication 800-30, Revision 1, Guide for Conducting Risk Assessments, September 2012
  + <https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final>
* NIST Special Publication 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, December 2018
  + <https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final>
* NIST Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, March 2011
  + <https://csrc.nist.gov/publications/detail/sp/800-39/final>
* NIST Special Publication 800-44, Version 2, Guidelines on Securing Public Web Servers, September 2007
  + <https://csrc.nist.gov/publications/detail/sp/800-44/version-2/final>
* NIST Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013
  + <https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final>
* NIST Special Publication 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations, September 2020
  + <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>
* NIST Special Publication 800-53A, Revision 1, Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans, December 2014
  + <https://csrc.nist.gov/publications/detail/sp/800-53a/rev-4/final>
* NIST Special Publication 800-53B, Control Baselines for Information Systems and Organizations, October 2020
  + <https://csrc.nist.gov/publications/detail/sp/800-53b/final>
* IST Special Publication 800-60, Volume 1, Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008
  + <https://csrc.nist.gov/publications/detail/sp/800-60/vol-1-rev-1/final>
* NIST Special Publication 800-60, Volume 2, Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices, August 2008
  + <https://csrc.nist.gov/publications/detail/sp/800-60/vol-2-rev-1/final>
* NIST Special Publication 800-61, Revision 2, Computer Security Incident Handling Guide, August 2012
  + <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>
* NIST Special Publication 800-115, Technical Guide to Information Security Testing and Assessment, September 2008
  + <https://csrc.nist.gov/publications/detail/sp/800-115/final>
* NIST Special Publication 800-128, Guide for Security-Focused Configuration Management of Information Systems, August 2011
  + <https://csrc.nist.gov/publications/detail/sp/800-128/final>
* NIST Special Publication 800-160 Volumne 1, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, November 2016
  + <https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final>
* NIST Special Publication 800-160 Volumne 2 (Draft), Developing Cyber Resilient Systems: A Systems Security Engineering Approach, September 2019
  + <https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/draft>
* Section 508 IT Accessibility Laws and Policies
  + <https://www.section508.gov/manage/laws-and-policies>

## Additional federal statutes

Review these for current versions and applicability

* Information Technology Management Reform Act of 1996 (Clinger-Cohen Act), 44 U.S.C 3501
* Computer Fraud and Abuse Act of 1986, 17 U.S.C 1201
* Computer Security Act of 1987, 44 U.S.C 3504
* Paperwork Reduction Act, 44 U.S.C. Chapters 29 and 35
* Freedom of Information Act (FOIA), as amended, 5 U.S.C. 552
* Privacy Act of 1974, 5 U.S.C. 552a
* Federal Records Act of 1950, as amended, 44 U.S.C. 2901
* Authority: Executive Branch Directives
* Homeland Security Presidential Directive 7
* Presidential Decision Directive 67 (PDD 67)