Acronym	Definition
AO	Authorizing Official A senior Federal official or executive with the authority to authorize (i.e., assume responsibility for) the operation of an information system or the use of a designated set of common controls at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation.
APT	Advanced Persistent Threat
BMA	Business Mission Area
CDD	Capability Development Document
CDSE	Center for Development of Security Excellence
CIA	Confidentiality, Integrity, Availability
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
CIO	Chief Information Officer The senior official that provides advice and other assistance to the head of the agency and other senior management personnel of the agency to ensure that IT is acquired and information resources are managed for the agency in a manner that achieves the agency's strategic goals and information resources management goals; and is responsible for ensuring agency compliance with, and prompt, efficient, and effective implementation of, the information policies and information resources management responsibilities, including the reduction of information collection burdens on the public.
CNSS	Committee on National Security Systems
CNSS 4009	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CNSSI 1253	Security Categorization and Control Selection for National Security Systems
CNSSP	Committee on National Security Systems Policy
CNSSP 22	Cybersecurity Risk Management Policy
CPD	Capability Production Document
Cybersecurity Framework	A risk-based approach to reducing cybersecurity risk composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers.

Acronym	Definition
DIMA	DOD portion of the Intelligence Mission Area
DOD	Department of Defense The DOD is an executive branch department of the federal government of the U. S. charged with coordinating and supervising all agencies and functions of the government concerned directly with national security and the United States Armed Forces. The major elements of these forces are the Army, Navy, Marine Corps, and Air Force.
DOD Instruction 8500.01	Cybersecurity
DOD Instruction 8510.01	Risk Management Framework (RMF) for DOD Information Technology (IT)
DODI	DOD Instruction
DSAWG	Defense IA/ Security Accreditation Working Group
EIEMA	Enterprise Information Environment Mission Area
Enterprise Architecture	A strategic information asset base, which defines the mission; the information necessary to perform the mission; the technologies necessary to perform the mission; and the transitional processes for implementing new technologies in response to changing mission needs; and includes a baseline architecture; a target architecture; and a sequencing plan.
FIPS	Federal Information Processing Standard
ICD	Initial Capabilities Document
Information Lifecycle	The stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition, to include destruction and deletion.
IS	Information System A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
ISO	Information System Officer An individual responsible for identifying all information types. An information type is considered any specific category of information defined by an organization or, in some instances, by a public law, executive order, directive, policy, or regulation.
ISRMC	Information Security Risk Management Committee

Acronym	Definition
ISSM	Information Security System Manager An individual appointed by a contractor with oversight responsibility for the development, implementation, and evaluation of the facility's information system security program. The ISSM must be trained to a level commensurate with the complexity of the facility's information systems.
ISSO	Information System Security Officer Individual with assigned responsibility for maintaining the appropriate operational security posture for an information system or program.
IT	Information Technology Any services, equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency. For purposes of this definition, such services or equipment if used by the agency directly or is used by a contractor under a contract with the agency that requires its use; or to a significant extent, its use in the performance of a service or the furnishing of a product. Information technology includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including cloud computing and help-desk services or other professional services which support any point of the life cycle of the equipment or service), and related resources. Information technology does not include any equipment that is acquired by a contractor incidental to a contract which does not require its use.
KS	Knowledge Service
MA	Mission Area
NISPOM Rule	National Industrial Security Program Operating Manual Rule
NIST	National Institute of Standards and Technology
NIST SP	National Institute of Standards and Technology Special Publication
NIST SP 800–30	Guide for Conducting Risk Assessments

Acronym	Definition
NIST SP 800–37	Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
NIST SP 800–39	Managing Information Security Risk: Organization, Mission, and Information System View
NIST SP 800–53	Security and Privacy Controls in Information Systems and Organizations
NIST SP 800–53A	Assessing Security and Privacy Controls in Information Systems and Organizations
NIST SP 800–60	Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices
NIST SP 800–137	Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
NIST SP 800–160	Developing Cyber Resilient Systems: A Systems Security Engineering Approach
NSS	National Security Systems
PAO	Principal Authorizing Official
PIT	Platform Information Technology
PM/SM	Program Manager/System Manager
RFP	Request for Proposal
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
Risk Assessment	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system.
Risk Management	The program and supporting processes to manage risk to agency operations (including mission, functions, image, reputation), agency assets, individuals, other organizations, and the Nation, and includes: establishing the context for risk-related activities; assessing risk; responding to risk once determined; and monitoring risk over time.

Acronym	Definition
RMF	Risk Management Framework Establishes a common set of guidelines for the assessment and authorization of ISs and provide a holistic and strategic process for the risk management of information systems.
SISO	Senior Information Security Officer
SP	Special Publication
STIG	Security Technical Implementation Guide
T&E	Test and Evaluation
TAG	Technical Advisory Group
WMA	Warfighting Mission Area