Glossary

Course: Continuous Monitoring

Authorization to Operate (ATO): The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

Authorizing Official (AO): A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations, (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Center for Development of Security Excellence (CDSE): The Center for Development of Security Excellence is responsible for providing security education and training to DoD and other U.S. Government personnel, DoD contractors, and sponsored representatives of foreign governments.

Chief Information Officer (CIO): The CIO leads the organization's Information Security Continuous Monitoring (ISCM) program. The CIO ensures that an effective ISCM program is established and implemented for the organization by establishing expectations and requirements for the organization's ISCM program; working closely with authorizing officials to provide funding, personnel, and other resources to support ISCM; and maintaining high-level communications and working group relationships among organizational entities.

Cognizant Security Agency (CSA): Agencies of the Executive Branch that have been authorized to establish an industrial security program to safeguard classified information when disclosed or released to U.S. Industry.

Configuration Item (CI): Items under a configuration management system.

Configuration Management Plan (CMP): Control details processes and procedures for how Configuration Management is used to support system development life cycle activities at the IS level.

Counterintelligence (CI): Defense Security Service (DSS) CI identifies threats to U.S. technology and programs resident in cleared industry and articulates that threat to stakeholders.

Defense Security Service (DSS): The Defense Security Service (DSS) is an agency of the Department of Defense (DoD) located in Quantico, Virginia with field offices

throughout the United States. The Under Secretary of Defense for Intelligence provides authority, direction, and control over DSS. DSS provides the military services, DoD Agencies, 30 federal agencies, and approximately 13,500 cleared contractor facilities with security support services. DSS is the Cognizant Security Office for most DoD classified contracts.

DSS supports the National Security and the warfighter, secures the nation's technological base, and oversees the protection of U. S. and foreign classified information in the hands of industry. DSS accomplishes this mission by clearing industrial facilities, accrediting information systems, facilitating the personnel security clearance process, delivering security education and training, and providing information technology services that support the industrial and personnel security missions of DoD and its partner agencies.

Developmental Test & Evaluation (DT&E): Testing that verifies that the system's design is satisfactory and that all technical specifications and contract requirements have been met.

Endpoint Protection Platforms (EPPs): Single endpoint solution that delivers antivirus, anti-spyware, personal firewall, application control, and other styles of host intrusion prevention.

Facility Security Officer (FSO): A U.S. citizen employee, appointed by a contractor who will supervise and direct security measures necessary for implementing the NISPOM and other federal requirements for classified information.

Global Information Grid (GIG): Globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel.

Information Owner (IO): Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

Information Security (IS): The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Information Security Continuous Monitoring (ISCM): Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

Information System Owner (ISO): Establishes processes and procedures in support of system-level implementation of the organization's ISCM program. This includes developing and documenting an ISCM strategy for the information system; participating in the organization's configuration management process; establishing and maintaining an inventory of components associated with the information system; conducting security

impact analyses on changes to the information system; conducting, or ensuring conduct of, assessment of security controls according to the ISCM strategy; preparing and submitting security status reports in accordance with organizational policy and procedures; conducting remediation activities as necessary to maintain system authorization; revising the system-level security control monitoring process as required; reviewing ISCM reports from common control providers to verify that the common controls continue to provide adequate protection for the information system; and updating critical security documents based on the results of ISCM.

Information System Security Manager (ISSM): 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.

Information System Security Officer (ISSO): ISSOs may be appointed by the ISSM in facilities with multiple accredited information systems. The ISSM will determine the responsibilities to be assigned to the ISSO in accordance with NISPOM Chapter 8.

Information System Security Professional (ISSP): Representative from the Office of Designated Approving Authority (ODAA) that provides advice and assistance visits to improve the security posture with regard to Information Systems and helps facilitate the process of getting your information systems accredited to process classified information.

Information Technology (IT): Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term *information technology* includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

Interim Authority to Operate (IATO): Temporary authorization granted for an information system to process information based on preliminary results of a security evaluation of the system.

Intrusion Detection and Prevention System (IDPS): Systems primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators.

Master System Security Plan (MSSP): Contains specific information to support a self-certification decision.

National Industrial Security Program (NISP): The National Industrial Security Program (NISP) was established by Executive Order 12829 for the protection of classified information released or disclosed to industry in connection with classified contracts. The NISP applies standards for the protection of classified information released or disclosed to contractors of all federal executive branch departments and agencies. Requirements of the NISP are stated in the National Industrial Security Program Operating Manual (NISPOM), (DoD 5220.22-M).

National Industrial Security Program Operating Manual (NISPOM): DoD Manual 5220.22-M issued in accordance with the NISP that prescribes the requirements, restrictions, and other safeguards for government contractors to prevent unauthorized disclosure of classified information.

National Institute of Standards and Technology (NIST): The federal technology agency that works with industry to develop and apply technology, measurements, and standards.

National Institute of Standards and Technology Special Publication (NIST SP): These publications provide guidelines for applying the Risk Management Framework and the development and implementation of an ISCM program that mitigates the threats and vulnerabilities to information systems.

Office of Designated Approving Authority (ODAA): Office within DSS that facilitates the certification and accreditations process for information systems at cleared contractor facilities.

Operating System (OS): A program that is loaded into the computer by a boot program that directs a computer's operations, controlling and scheduling the execution of other programs, and managing storage, input/output, and communication resources.

Operational Test & Evaluation (OT&E): Follows DT&E and validates that the system under test can effectively execute its mission in a realistic operational environment when operated by typical operators against representative threats. The difference between DT&E and OT&E is that DT&E verifies that the system is built correctly in accordance with the specification and contract, and OT&E validates that the system can successfully accomplish its mission is a realistic operational environment.

Plan of Action and Milestone (POA&M): A document that reports progress on items in SSP, identifies vulnerabilities, and addresses action to reduce, eliminate, or accept those vulnerabilities.

Platform Information Technology (PIT) Systems: A collection of PIT within an identified boundary under the control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location.

Principal Authorizing Official (PAO): Senior official with authority and responsibility for all systems within an agency.

Protection Level 1 (PL-1): An indication of the implicit level of trust that is placed in a system's technical capabilities and is based on the classification and sensitivity of information, clearances, formal access approvals, and the need-to-know. PL-1 indicates that all users are cleared, all users have access, and all users have a need to know.

Public Key Infrastructure (PKI): The framework and services that provide for the generation, production, distribution, control, accounting, and destruction of PK certificates.

Risk Management Framework (RMF): A common information security framework developed to improve information security, strengthen risk management processes, and encourage reciprocity among federal agencies.

Security Assessment Report (SAR): A report containing the assessment and characterization of the aggregate level of the risk to the system, based on the determined risk level for each non-compliant security control.

Security-focused Configuration Management (SecCM): The management and control of configurations for information systems.

Security Impact Analysis: Analysis performed by organizational personnel with information security responsibilities to analyze changes to the IS to determine potential security impacts prior to change implementation.

Security Training Education and Professionalization Portal (STEPP): The learning management system used by the Center for Development of Security Excellence (CDSE). STEPP is where the list of courses is maintained and where student information and course transcripts are maintained.

Senior Information Security Officer (SISO): Establishes, implements, and maintains the organization's ISCM program; develops organizational program guidance (i.e., policies/procedures) for continuous monitoring of the security program and information systems; develops configuration management guidance for the organization; consolidates and analyzes POA&Ms to determine organizational security weaknesses and deficiencies; acquires or develops and maintains automated tools to support ISCM and ongoing authorizations; provides training on the organization's ISCM program and process; and provides support to information owners/information system owners and common control providers on how to implement ISCM for their information systems.

System Security Plan (SSP): A formal agreement that specifies the security requirements, describes security controls, and contains security-related documents (e.g., risk assessment, contingency plan, incident response plan, interconnection agreements).