Glossary and Acronyms

Annual Assessment (AA)

After an initial SA&A package is completed, an annual assessment is conducted to review specific security controls identified by the agency each year, and to review outstanding plan of action and milestone (POA&M) weaknesses that remain from prior assessments and from any ongoing testing that has been conducted during the previous reporting year.

Assessment and Authorization (A&A)

The FISMA Assessment and Authorization (A&A) (formerly known as Certification and Accreditation (C&A) and Security Assessment & Authorization (SA&A)) is the formal process of evaluating, testing, and examining security controls that have implemented in an information system by using the Security Control Assessment process as described in NIST 800-37 (Risk Management Framework). Authorization (previously known as accreditation), is the formal written authorization by for a system to operate. The authorizing official (or designated approving/accrediting authority as referred to by some agencies) is a senior management official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations, agency assets, or individuals. Assessment and Authorization map to steps 4 and 5 of the NIST Risk Management Framework, respectively.

Authority to Operate (ATO)

An ATO is a formal declaration by an authorizing official (AO), who authorizes operation of a system and explicitly accepts the risk to agency operations. The ATO is signed after a security assessor certifies that the system has met and passed all requirements to become operational.

Authorizing Official (AO)

The AO is an federal official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. The AO can include, but is not limited to: Chief Information Officer, Chief Information Security Officer, Information System Security Officer, Center/Office/Division Director or Deputy Director, or a Project Officer. The role of authorizing official has inherent U.S. Government authority and is assigned to government personnel only.

Cloud Service Provider (CSP)

A service provider that offers customers Platform as a Service (PaaS), Infrastructure as a Service (IaaS), or Software as a Service (SaaS), available via a private, public, or hybrid deployment models. See NIST 800-145 for more information on the Cloud Service Provider Definition, service models, and deployment models.

Continuous Diagnostics and Mitigation (CDM)

The Department of Homeland Security (DHS) CDM program provides capabilities and tools that enable network administrators to know the state of their respective networks at any given time, including relative risks and threats, and helps system personnel to identify and mitigate flaws at near-network speed. The CDM program enables government entities to expand their continuous diagnostic capabilities by increasing their network sensor capacity, automating sensor collections, and prioritizing risk alerts.

Continuous Monitoring (CM)

Systems enter the CM Phase (Step 6 of the NIST RMF) after achieving ATO. The purpose of this phase is to provide oversight and monitoring of the security controls in the information system on an ongoing basis and to inform the Authorizing Official (AO) when changes occur that may impact the security of the system. CM consists of three tasks: (i) configuration management and control; (ii) security control monitoring; and (iii) status reporting and documentation, which are performed continuously throughout the life cycle of an information system.

Control Baseline

The set of security and privacy controls that are applicable to information or an information system to meet legal, regulatory, or policy requirements, as well as address protection needs for the purpose of managing risk. The control baseline is developed during Step 2 (Select) of the RMF.

E-Authentication Risk Assessment (eRA) / e-Authentication Threshold Analysis (eTA)

The e-Authentication initiative describes trusted, secure, standards-based, interoperable authentication architecture. This initiative has been developed to provide a uniform process for establishing electronic identity to support the President's Management Agenda (PMA) of 2002 and the E-Government Act of 2002. The e-Authentication initiative eliminates the need for each agency to develop a redundant solution to verify an individual's identity and to support electronic signatures. The e-Authentication Risk Assessment process provides a systematic process by which system/information owners assess relative security impacts across multiple threat areas, to determine the appropriate authentication and identity proofing requirements for their system. The e-Authentication process generates an e-authentication assurance level (EAL) rating (i.e., 1-4), which can then be mapped against guidance in NIST 800-163 to determine the appropriate authentication technology and identity proofing requirements.

Enterprise Performance Life Cycle (EPLC)

PLC is HHS's framework to enhance Information Technology (IT) governance through rigorous application of sound investment and project management principles and industry best practices. The HHS EPLC provides the context for the HHS IT governance process and describes interdependencies between its project management, investment management, and capital planning components. EPLC and the System Development Life Cycle (SDLC) are sometimes used interchangeably, but there are differences between the two models. You should visit the HHS EPLC Page for more information by visiting: https://ocio.nih.gov/PM/Pages/EPLC.aspx

Federal Information System

The U.S. Office of Management and Budget (OMB) describes a federal information system (sometimes called a federal application) as a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual. (Defined in OMB circular A-130, (6)(q)). Further, OMB has clarified that Federal Information Systems are those that are used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency (44. U.S.C. § 3544(a)(1)(A)). The definition of a system can sometimes be unclear or misinterpreted. If you are unsure whether yours qualifies as a federal information system, please contact the NCI ISSO at NCIIRM@mail.nih.gov for help in making a final determination.

Federal Information Security Modernization Act (FISMA) of 2014

The Federal Information Security Modernization Act of 2014 (Public Law No: 113-283 (12/18/2014) - amends the Federal Information Security Management Act of 2002. The act recognizes the importance of information security to the economic and national security interests of the United States. FISMA requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. FISMA is the law that drives all agency A&A related compliance activities.

Federal Risk and Authorization Management Program (FedRAMP)

FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. The FedRAMP assessment process is initiated by agencies or cloud service provider (CSPs) beginning a security authorization process using the FedRAMP requirements which are FISMA compliant and based on the NIST 800-53 (as amended) and initiating works with the FedRAMP Program Management Office (PMO), based out of the General Services Administration (GSA).

Federal Information Processing Standards 199 (FIPS-199) Security Categorization

The FIPS-199 Security Categorization process addresses the first task required by the Risk Management Framework (RMF) to develop standards for categorizing information and information systems. The FIPS-199 publication from NIST establishes security objectives for both information and information systems on Confidentiality, Integrity, and Availability as well as defines correlating potential impact levels of Low, Moderate, and High. Security categories (security objective + impact level) are then derived based on the potential impact on each of the Confidentiality, Integrity, and Availability of information and information systems within an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization. The security categorization is the collection of all security categories for all security objectives and is recorded on the FIPS-199 form. NCI uses the high watermark approach, so the overall categorization of the system is the equivalent to the highest individual security category(ies).

High Water Mark

For an information system, the potential impact values assigned to the respective security objectives (confidentiality, integrity, availability) shall be the highest values (i.e., high water mark) from among those security categories that have been determined for each type of information resident on the information system. So for example a system rated M-L-L, L-M-L, M-M-L, etc. would all be rated Moderate overall since Moderate is the highest rated security objective.

Low-Impact Software-as-a-Service (LI-SaaS) Approval

To use cybersecurity as an enabler in the NCI research enterprise, the NCI Chief Information Security Officer (CISO) and Chief Information Officer (CIO) will consider requests to authorize certain innovative cloud services if they are low risk (i.e., rated Low impact using the FIPS-199 process) and are classified as software as a service (SaaS) cloud offering. The low impact SaaS (LI-SaaS) review and authorization is intended to streamline the authorization necessary for the federal government to use a SaaS product (1) when the cloud service provider does not have and is not willing to obtain a FedRAMP authorization, and (2) when the product is not listed on or eligible to be approved as Third Party Websites and Applications (TPWA). TPWA's are a special category of no-cost (free) online services and products, and when approved by HHS are placed on the list of HHS-approved TPWAs. See the LI-SaaS Review/Approval Process and Approved SaaS Cloud Products Knowledge Article for more information.

NIH Security Assessment Tool (NSAT)

NSAT is NIH's central repository and tracking tool for all FISMA assessment and authorization (A&A) information and artifacts. All NIH operated systems and some externally operated systems are required to store their information directly in NSAT to help automate information gathering and streamline reporting. Contact your ISSO to find out if your system needs to be entered into NSAT.

Plan of Action and Milestones (POA&M)

The POA&M is a summary of findings and weaknesses from the security assessment and from ongoing (continuous) security monitoring activities. The POA&M details resources (e.g., time, money) required to accomplish the objectives of the plan, any milestones in meeting the objectives, and scheduled completion dates. The purpose of this POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.

Privacy Impact Assessment (PIA)

The PIA is an analysis of how privacy information related to a federal information system is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Risk Assessment (RA)

Risk Assessment is the process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals arising through the operation of the information system. Part of risk management, synonymous with risk analysis, incorporates threat and vulnerability analyses, and considers mitigations provided by planned or in place security controls.

Risk Management Framework (RMF)

The RMF describes a six-step structured, yet flexible approach that can be used to determine the appropriate level of risk mitigation needed to protect the information systems, information, and infrastructure supporting organizational mission/business processes from serious threats. These steps include: 1) Categorize the information system; 2) Select security controls; 3) Implement security controls; 4) Assess security controls; 5) Authorize the information system; and 6) Monitor security controls. The RMF is designed to guide organizations in developing good practices for securing their information and information systems by helping leadership understand the current status of its security programs and the security controls planned or in place to protect Federal information and information systems in order to make informed judgments and investments that appropriately mitigate risk to an acceptable level. The RMF provides a methodology that can be applied in an iterative manner to both new and legacy information systems within the context of the system development life cycle (SDLC) and the Federal Enterprise Architecture (FEA). For each of the six steps of the framework, NIST has developed standards and guidance to enable organizations to effectively apply the framework to the information systems supporting the organization's mission/business processes. The RMF is defined in NIST Special Publication 800-37 rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*.

Security Assessment Report (SAR)

The Security Assessment Report documents an assessment team's results of the security control assessment. The assessment team reports, for each assessment procedure performed, whether each determination statement in an assessment procedural step was "satisfied" or "other than satisfied." In the latter case, the assessment team indicates which parts of the security control were affected by the finding, describes how the control differs from the planned or expected state, and notes any potential compromises to confidentiality, integrity, and availability due to the "other than satisfied" result.

Security Control Assessor

The security control assessor (SCA) is the individual, group, or organization responsible for conducting a comprehensive assessment of the management, operational, and technical security controls employed within or inherited by an information system to determine the overall effectiveness of the controls (i.e., the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system). Security control assessors also provide an assessment of the severity of weaknesses or deficiencies discovered in the information system and its environment of operation and recommend corrective actions to address identified vulnerabilities.

Security Impact Analysis (SIA)

A security impact analysis is conducted in the continuous monitoring phase after a system receives an ATO when the system is planning to undergo a significant change which may impact the security posture of the system. The SIA process analyzes significant changes to the information system to determine potential security and privacy impact prior to change implementation. An SIA must be completed and approved before a new significant change, upgrade, or release is deployed to the production environment.

Significant Change

A significant change as defined in the NIST Special Publication 800-37 Rev. 2 *Risk Management Framework for Information Systems and Organizations*, is a change that is likely to substantively affect the security or privacy posture of a system. Depending on the type of significant change to a system it can trigger one of two processes: 1) the completion and approval of a SIA or 2) re-authorization of the system.

Examples of significant changes to a system that may trigger an **SIA** may include, but not limited to:

- Installation of a new or upgraded operating system, middleware component, or application;
- Modifications to system ports, protocols, or services;
- Installation of a new or upgraded hardware platform;
- Modifications to how information, including PII, is processed;
- Modifications to cryptographic modules or services;
- Changes in information types processed, stored, or transmitted by the system; or
- Modifications to security and privacy controls.

Significant changes to the environment of operation that may trigger a **re-authorization** action may include, but are not limited to:

- Moving to a new facility or operating environment;
- Adding new core missions or business functions;
- Acquiring specific and credible threat information that the organization is being targeted by a threat source; or
- Establishing new/modified laws, directives, policies, or regulations.

Special Purpose Equipment (SPE)

Equipment which is used only for research, medical, scientific, or other technical activities. Examples of special purpose equipment include microscopes, x-ray machines, surgical instruments, and spectrometers.

System Security Plan (SSP)

The SSP is the formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.

Systems Development Life Cycle (SDLC)

SDLC, also referred to as the application development life-cycle and the Enterprise Performance Life Cycle (EPLC), is a term used in systems, information systems, and software engineering to describe a process for planning, creating, testing, and deploying an information system. The SDLC concept applies to a wide range of hardware and software configurations.