FISMA FAQ

What is SA&A?

The Security Assessment and Authorization (SA&A) process (formerly known as Certification & Accreditation (C&A)) is described in the National Institute of Standards and Technology (NIST) Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems. The guiding principle of SA&A is continuous risk management in which security measures are constantly evaluated and addressed to meet evolving security threats. This continuous monitoring strategy will help with the continual evaluation and re-authorization of systems by using increased security automation resources.

The result of a successful SA&A is an authorization to operate (ATO) for the subject information system or application being reviewed. By law, each authorization can be valid for up to 3 years depending upon whether significant changes occur to the system following an ATO. NIST 800-37 stresses the importance of a continuous monitoring (CM) strategy that will help with the continual evaluation and re-authorization of systems that already have their ATO, by using increased security automation resources.

How does SA&A benefit my system?

SA&A is a process by which system owners can demonstrate their compliance in regard to protecting the confidentiality, integrity, and availability of federal systems and information. The federal government implemented the SA&A requirement as part of the Federal Information Systems Modernization Act (FISMA) of 2014 to help ensure and demonstrate that federally owned and/or operated systems and federal data are secured using a risk based approach.

Government networks and systems face growing and relentless cyber-attacks by individuals, private organizations, and state-sponsored entities. Because NIH is known to collect, store, and process valuable scientific and clinical-research data, the agency is a ripe target for certain malicious individuals and groups. Even publicly disseminated data that are freely distributed by NIH need to be accurate, timely, and reliable; therefore, public data collections also require robust security measures.

How do I know whether my system requires a SA&A?

According to the Federal Information Security Management Act (FISMA), all information systems that collect, store, or process federal information are subject to the SA&A requirement. This includes, but is not limited to Federal systems hosted at federal facilities, contractor or subcontractor facilities, third-party hosted data centers, research facilities, and cloud-service providers.

Does FISMA apply to Grants and to Cooperative Research and Development Agreements (CRADA)?

The current regulations are pursuant to the Federal Information Security Management Act (FISMA), 44 U.S.C. 3541 et seq. The applicability of FISMA to NIH grantees applies only when grantees collect, store, process, transmit or use information on behalf of HHS or any of its component organizations. In all other cases, FISMA is not applicable to recipients of grants, including cooperative agreements. The grantee retains the original data and intellectual property, and is responsible for the security of this data, subject to all applicable laws protecting security, privacy, and research. If and when information collected by a grantee is provided to HHS, responsibility for the protection of the HHS copy of the information is transferred to HHS and it becomes the agency's responsibility to protect that information and any derivative copies as required by FISMA. For the full Grants policy, please visit the NIH Grants policy page here (link is external).

Do I need to complete any NCI-required security forms?

Yes. Federal Information Processing Standards (FIPS) 199 and E-Authentication Threshold Analysis (ETA)/E-Authentication Risk Assessment (ERA) forms are required. Refer to the NCI Starter Kit page for further information about these forms and how to submit them to the NCI ISSO. You may also need to complete a Privacy Impact Assessment (PIA).Visit the Starter Kit page for more information and to determine when a PIA is or is not required.

My system operates out of an offsite, non-government-owned facility or in the cloud; does it still require an SA&A and a formal authorization to operate (ATO)?

Yes, if the system meets the criteria that define a federal information system, then it does need an SA&A and an ATO. If you are responsible for a system that is hosted outside an NIH-owned or NIH-operated facility, you should consult with the NCI ISSO (link sends email).

for specific guidance to make sure you're properly complying with FISMA regulations. You should also coordinate with your respective Contracting Officer Representative (COR) for contract related questions, and with your grants administrator if operating under a grant. Keep in mind that systems or applications that live within an existing authorization boundary of a Major Application or General Support System may inherit an authorization. See the FAQ below regarding authorizations within authorized Major Application or GSS systems.

Can you provide an overview of the SA&A process?

NCI and NIH follow the NIST Special Publication 800-37 rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. You should adhere to the 800-37 rev. 2 RMF and use templates published by the NIST under the 800 series of NIST special publications.

When should I start the SA&A process?

Because the Federal Information Security Modernization Act (FISMA) of 2014(link is external) requires that all federal information systems have a written authority to operate (ATO) by the time the system is deployed into production, you should begin preparing for the SA&A as soon as the system has been approved for acquisition or development. If your system is already in production and doesn't have an ATO — this is often the case with legacy systems—it is still important to start the SA&A process as soon as possible to avoid the possibility that you might be required to take it offline until an ATO has been issued.

How long does it take to complete a Security Assessment and Authorization (SA&A)?

Rough estimates include:

- Low impact systems: 1-2 months
- Moderate impact systems: 2-3 months
- High impact systems: 3-5 months

These estimates will vary based on variables including the size and complexity of the system, the experience of the SA&A assessor, and how well the system owner and system team have prepared for the SA&A.

Who are NCI's points of contact for SA&A support, and for security compliance guidance?

You should coordinate SA&A activities with your Contracting Officer Representative (COR) and NCI project/program manager. If you still have questions after speaking with your COR or PM, you can email the NCI ISSO (link sends email).

Who pays for the SA&A?

The responsible government project sponsor must ensure that adequate funding is allocated to support all security-related compliance activities, including FISMA and the SA&A. Responsible individuals should plan accordingly in their operating budgets as well as in all IT-related acquisition plans.

The government sponsor or business owner needs to factor in ongoing security expenses arising from conducting continuous monitoring, maintaining and updating security-related system documentation, and addressing weaknesses identified through ongoing assessments. Excluding the initial SA&A expense, the ISSO recommends that system owners should set aside roughly 3-5% of their system's annual operating budget for security and compliance activities.

Can I conduct the SA&A myself?

You can conduct the SA&A if your system is rated LOW impact, using to the criteria contained in the Federal Information Processing Standards 199 (FIPS-199) assessment framework. If you conduct it yourself, you still must adhere to the National Institute of Standards and Technology (NIST) 800-37 Risk Management Framework (RMF) for conducting the assessment. Systems that are rated moderate or high must be reviewed by an independent assessor. Read NIST 800-37 Section 3.4(link is external) for a detailed description on how to determine appropriate assessor independence.

What do I do about SA&A security findings?

All findings identified in the SA&A should be remediated completely, addressed through compensating controls, or accepted in writing by the authorizing official according to the Office of Management and Budget (OMB). Any exceptions to NIH policy must be approved by the NCI Information Systems Security Officer (ISSO) and the NIH Chief Information Security Officer (CISO) using the standard security-waiver form.

If you have questions about risk acceptance memos or security waivers, contact the NCI ISSO (link sends email).

Who is my Authorizing Official/Designated Approving Authority (AO/DAA)?

The AO/DAA is the official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. In the case of externally hosted systems, this is most likely your government program manager or COR. You should speak with your COR to verify who will act as your system's AO.

What is FedRAMP?

The Federal Risk and Authorization Management Program, or FedRAMP, is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a "do once, use many times" framework that saves an estimated 30-40% of government costs, as well as both time and staff required to conduct redundant agency security assessments. Visit http://www.fedramp.gov/(link is external) for more information.

Does FedRAMP apply to my system?

If you currently, or if you plan to, host an NCI IT system - and any Federal IT system for that matter - in the cloud, then FedRAMP most likely does apply. FedRAMP is mandatory for federal agency cloud deployments and service models. Private cloud deployments intended for single organizations and implemented fully within federal facilities are the only exception. You should consult with your IC ISSO to determine if FedRAMP applies to your situation and for guidance on how to identify FedRAMP certified cloud service providers (CSP).

How do I determine if my cloud service provider is FedRAMP certified?

For the latest list of cloud providers that are FedRAMP certified, visit the FedRAMP Marketplace.

If my system is part of an existing major application (MA) or general support system (GSS), do I still need an SA&A?

This depends on whether the Major Application or General Support System has its own authorization to operated, which it should. If your application resides within an existing authorization boundary and shares a significant number of security controls of that boundary system, then it may inherit the security authorization. This question should always be addressed with your ISSO. Remember, all systems require an authorization to operate, but how that is implemented may vary on a case by case basis. Even if your application inherits an ATO, you will be required to provide a minimum set of documentation and potentially subject your system to automated security scanning and analysis to ensure your application does not alter or adversely impact the overall risk posture and authorization of the parent authorization.

What if my system doesn't receive an authorization to operate (ATO)?

An Authorization to Operate (ATO) is a formal declaration by an Authorizing Official that authorizes operation of an information system and explicitly accepts the risk to agency operations. The ATO is signed after a security control assessor certifies that the system has met and passed all requirements to become operational. If your ATO is denied, you will need to remedy unacceptable risks before submitting another ATO request. The NIH and the Office of Management and Budget, do not currently recognize interim authority to operate (IATO) only an ATO.

Do I have any SA&-related responsibilities during the time between assessments?

Yes. Most importantly, you will need to address any weaknesses that have been identified and documented in your system's Plan of Action and Milestones (POA&M) and address application and website specific vulnerabilities that may be discovered through required ongoing automated scans. Your up-to-date POA&M may be requested by the NCI ISSO at any time so it is important to keep it current and to proactively address all documented findings.