Mass General Brigham

Federal Sponsored Research Contracts with Information Security Terms (FedRAMP)

November 2021

Overview: This SOP sets forth a process for identification, review, and implementation of technical security requirements throughout the lifecycle of federal contracts and subcontracts with FedRAMP clauses. Please see the FISMA SOP for federal contracts with FISMA (Federal Information Security Management Act) terms.

I. What are FedRAMP Information Security (IS) Terms?

- *IS Terms may be referenced as "FedRAMP" or* DFARS Clause 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting) in a federal contract or subcontract.
- These terms are not the same as FISMA terms.
- FedRAMP requires technical security or procedures that are not standard for Mass General Brigham institutions and their annual IS reports to federal sponsors, employee rosters, training and/or background checks. In addition, FedRAMP IS requirements also apply to cloud services such as Infrastructure as a Service (IAAS), Platform as a Service (PAAS), and Software as a Service (SAAS). Please consult with ERIS if you need assistance with Cloud models (rcc@partners.org).
- FedRAMP terms require specific technical expertise that is available to Research projects for a fee through the Mass General Brigham (MGB) Research IT Core. If allowed by the sponsor, the cost for these services should be included in the proposal budget, as described below, or covered by Sundry or department funds.
- MGB Research IT Core costs and services are available here: https://rc.partners.org/research-apps-and-services/security/fisma-security-documentation#budget-guide.

II. Proposal Stage

A. Department Review

1. When submitting a federal Prime contract proposal through an MGB institution or a federal subcontract proposal through an external entity serving as the Prime Contractor, the MGB Principal Investigator (PI) is responsible for reviewing the contract's Request for Proposal (RFP) for FedRAMP Terms.
2. If there are FedRAMP terms, the MGB PI should proceed as follows:
    - **Contact Brent Richter of the MGB Research IT Core for an assessment and FedRAMP plan prior to submitting the proposal to Pre-Award**. Additionally, the Cloud Service Provider (CSP) and 3rd Party Assessment Organization (3PAO) must be engaged. For a fee, the Core will assist with defining and developing the security documentation required for

FedRAMP. All Core costs should be included in the proposal budget. If deemed an unallowable cost by the sponsor, Core fees must be covered by departmental or Sundry funds. When preparing the budget, the PI should also include cloud service costs and security tools required for compliance. Some contracts may require submission of an initial self-assessment and/or risk assessment with the proposal. These can be obtained from the MGB Research IT Core.

- Alternatively, and in rare instances, the PI may identify departmental staff with the appropriate technical expertise who can implement the required procedures and complete technical reports. To use departmental staff:
    a. The PI must receive approval from Fabio Martins, the MGB Information Security Officer (RISO) and the hospital Information Security Officer (ISO) confirming the proposed individual(s) has the requisite expertise. The MGB Research IT Core must review and sign-off on any department-generated required technical reports prior to sponsor submission.
    b. The PI may not rely on department staff for contracts or subcontracts with information security accreditation or certification requirements. In these instances, the PI must use the MGB Research IT Core. **Authorization to sign accreditation or certification is limited to Brent Richter.**

B. Research Management Pre-Award Review

1. The Pre-Award Grant administrator (GA) will review the terms of all contract or subcontract RFPs for IS Terms and, if found, consult with the Pre-Award Director and Director for Contracts. The review will include terms for FedRAMP specifically as Referenced in RAR 1.1-3. The GA will then confirm that both the DA and PI are aware of the IS terms and have budgeted for the use of the Mass General Brigham Research IT core, including the CSP costs, or confirmed the use of alternate paths with the Mass General Brigham RISO and hospital ISO, as above. The Agreement Associate (AA) will also review the IS Terms and negotiate with the sponsor, if required at proposal stage.
2. Any reports or certifications submitted with the proposal to federal sponsor's Chief Public Affairs Officer (CPAO) or other designated official must be uploaded to the Insight Agreements Module.

III. Contract Negotiation

1. Prior to contract execution, the AA reviews the contract or subcontract for FedRAMP IS Terms.
2. If FedRAMP Terms have been included, the AA notifies the PI and informs Brent Richter that a contract/subcontract with FedRAMP requirements has been received. The AA also notifies the site's Director of Research Compliance. The 3PAO and the CSP along with the FedRAMP PMO must be included in the contract negotiation. *Note: Negotiators should understand timing and dependencies required for provisional or final Authority To Operate (ATO).*
3. Prior to contract execution, the PI, RISO, hospital ISO, and MGB Research IT Core review implementation of the FedRAMP requirements as well as the plan submitted with the proposal. They

also confirm the PI's funding mechanism, i.e., charging the contract or Sundry or departmental funds. Final approval from Brent Richter confirming that the requirements have been met to date and can continue to be met is necessary before the contract is signed.

IV. Contract Compliance

A. FedRAMP Personnel Requirements

If the contract/subcontract includes personnel requirements (e.g., onboarding, training, or termination), the PI and their designee are responsible for complying with these requirements. This includes staff involvement from the CSP and 3PAO (See Appendix A).

B. Annual Reporting

1. On an annual basis, the PI is responsible for contacting Brent Richter of the MGB Research IT core, Fabio Martins (RISO), and the hospital's ISO 90 days prior to the date annual reports are due in order to prepare and submit any required reports under the FedRAMP Terms.
2. Copies of the final report(s) must be uploaded to the Insight Agreements Module.

V. Roles & Responsibilities

	Pi	Dept Admin	Pre Award GA	Post Award Ga	Agmt. Assoc	Research IT Core	Hospital ISO	MGB RISO	3Pao	CSP
Review terms of all RFPs for IS Terms	X	X	X							
Confirm PI is aware of special requirements in IS Terms	X	X	X							
Engage 3Pao, CSP, and FedRamp PMO (if required)	X	X	X							
Negotiate IS Terms in proposal with Sponsor, if necessary (authorization approach etc)					X	X				
Negotiate Terms with 3PAO and CSP to consider IS Terms as per the proposal requirements					X	X				
Confirm resources and work in conjunction with MGB to identify 3PAO (if required) and to provide necessary documentations as per FedRAMP compliance requirements.										X
Confirm resources and provide updates to MGB about authorization schedule and plan for the assessment including appropriate documentation and reporting as per FedRAMP requirements								X		
Complete reports or certifications required at proposal	X	X	X			X				
Upload reports or certifications required at proposal to InfoEd	X	X	X							
Budget for use of MGB Research IT Core in proposal – Considering the cost of 3PAO and CSP Resources	X	X	X							
[Rarely] Approve use of department staff to meet contract – To include FedRAMP requirements						X	X	X		
Review and confirm compliance with IS Terms prior to contract signature	X				X	X				
Ensure compliance with ongoing Personnel training and roster requirements	X	X				X				
Contact MGB Research IT Core and Partners RISO 90 days prior to annual report and/or security plan update due date	X	X				X				
Prepare annual reports/security plan updates & secure approval of updates from MGB Research IT Core	X	X								
Submit to sponsor /prime with a copy to Research Management Post-Award for uploading to InfoEd	X	X		X						
Provide Updates on a yearly basis to SSP (Both SSP and PI)	X	X								X