Information Security FISMA Compliance Process

Overview

The Federal Information Security Management Act (FISMA) is a United States federal law enacted to ensure the security of government-owned information. FISMA requires each federal agency to develop, document, and implement a program to provide information security for the information and information systems that support the operations and assets of the agency, including those that are managed by an outside source. This means that, under some Federal contracts, information the University of Rochester (UR) collects or stores will need to comply with FISMA compliance.

Contracts are reviewed by the Office of Research and Project Administration (ORPA) for budgetary obligations and possible information security requirements. In the context of FISMA, the term 'information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure the confidentiality, integrity, and availability of the data. Once the review is completed by ORPA, a meeting is set between the principal investigators (PI) and ORPA to review the contract obligations. It is the responsibility of the PI to ensure FISMA compliance at the onset of the contract as well as throughout the contract duration. During the initial meeting with ORPA, the PI should be made aware of the risk level associated with the contract as dictated by NIH.

FISMA compliance is required only for those contracts that contain compliance requirements within the contractual language. To date, UR has accepted contracts with the National Institutes of Health (NIH) that require compliance under FISMA guidelines. It is important that researchers identify FISMA or other information security requirements as early in the contract process as possible. This will ensure that all FISMA-related data remains secure.

As part of FISMA compliance, an Information Technology Security Plan (IT-SP) is filed with NIH at the determined intervals. UR generates the IT-SP in order to assure NIH that data provided by and to NIH is kept sufficiently secure and is not released to any person not permitted to access the data, either through malicious or inadvertent means. The scope of the IT-SP includes the contracted group performing the research and any associated supporting infrastructure. The security responsibilities are a collaborative effort between the University of Rochester and the PI.

Verification of the compliance of the security controls is completed by the office of University Audit (OUA) on an annual basis. OUA independently evaluates the compliance of the security controls and develops a corrective action plan as needed.

Information Technology Security Plan

The security controls included in the IT-SP are based up on the National Institute of Standards and Technology (NIST) SP 800-53 Rev 4 control framework. The NIST framework contains the following control categories:

- Access Control
- Awareness and Training
- Audit and Accountability
- Certification, Accreditation, and Security Assessments

- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection
- Planning
- Personnel Security
- Risk Assessment
- System and Service Acquisition
- System and Communication Protection
- System and Information Integrity

The PI should work with ORPA to identify the information security controls that are required as part of the contract. The administration of the information security controls is the responsibility of the PI. Once the FISMA security requirements are identified, the PI should complete the FISMA Information Security Work Request and submit it to the Information Security Risk and Compliance Director. This work request will result in a meeting with an Information Security representative to discuss the security controls in place and if any additional requirements need to be met by the PI. Required controls are determined by the risk level associated with the contract.

Once the risk assessment and control inventory are completed, a meeting will be set up by Information Security to discuss the security controls currently in place with the PI. At this meeting the PI will be notified of all existing security controls managed by UR Information Security as well as any additional controls that are the responsibility of the PI. The PI will be provided a control inventory for all security controls managed by Information Security and an IT-SP for those controls. Based on FISMA contract requirements, this process will need to be completed annually at the request of the PI with appropriate notification time.

Working with Information Security

Once the existence of the FISMA information security requirements is identified, the PI should complete a FISMA work request form and submit it to the Information Security Risk and Compliance Director. The work request will be completed in no less than 30 days from acceptance by Information Security and will require the following information:

- Contract Name
- Name of Principal Investigator
- Alternate contact
- Risk Level assigned by NIH
- Start Date of Contract
- End Date of Contract
- Systems that will be used (both UR-managed and Non UR-managed)
    - ➢ Network location
    - ➢ Server name(s)

  - Application(s)
  - Database(s) in use
  - Personal computing device(s)
  - Data storage location(s)
- Copy of the grant to ensure the proper security controls are being assessed

The work request form can be obtain from ORPA or by contacting the Information Security Risk and Compliance group.

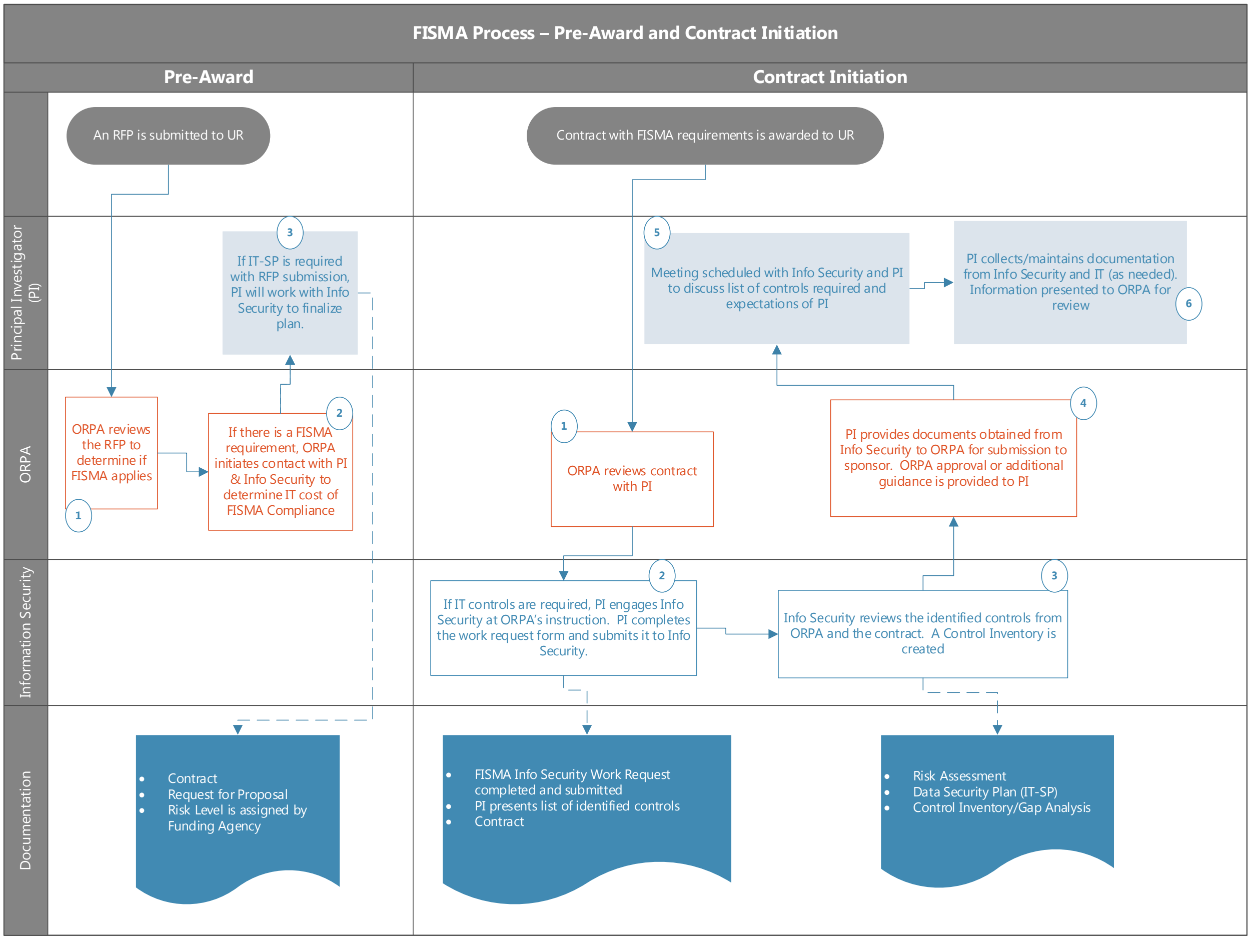
The FISMA work request will result in a risk assessment of the security controls currently in place pertaining to the systems and storage locations indicated on the work request form. If additional storage locations are in use but not disclosed, the security controls associated with those additional locations will be outside of this review. Once the risk assessment is complete, a meeting will be scheduled by Information Security Risk and Compliance with the PI to discuss the findings of the risk assessment, any additional requirements that the PI must actively address, and the completed control inventory. While Information Security will attest to the security measures in place on UR managed systems, ensuring of FISMA compliance requirements are met is the responsibility of the PI.

FISMA Work Request

Contract Name		
Principal Investigator		
Alternate Contact		
Department Performing Research		
NIH Assigned Risk Level		
Start Date of Contract		
End Date of Contract		
System Information:		
Server Name		
UR-Managed Server	Yes	No
Location of Server		
Devices in use	Android	Mac
Where is back up data stored?		
Is this a new FISMA Contract	Yes	No
Has a copy of the contract been included?	Yes	No
Requested Completion Date		
Has a copy of the contract been attached to this request?	Yes	No

FISMA-related work requests will be completed by an Information Security representative in no less than 30 days from the date request is Accepted by Risk and Compliance Manager

FISMA Process – Pre-Award and Contract Initiation



Pre-Award

An RFP is submitted to UR

1 ORPA reviews the RFP to determine if FISMA applies

2 If there is a FISMA requirement, ORPA initiates contact with PI & Info Security to determine IT cost of FISMA Compliance

3 If IT-SP is required with RFP submission, PI will work with Info Security to finalize plan.

- Contract
- Request for Proposal
- Risk Level is assigned by Funding Agency

Contract Initiation

Contract with FISMA requirements is awarded to UR

1 ORPA reviews contract with PI

2 If IT controls are required, PI engages Info Security at ORPA's instruction. PI completes the work request form and submits it to Info Security.

3 Info Security reviews the identified controls from ORPA and the contract. A Control Inventory is created

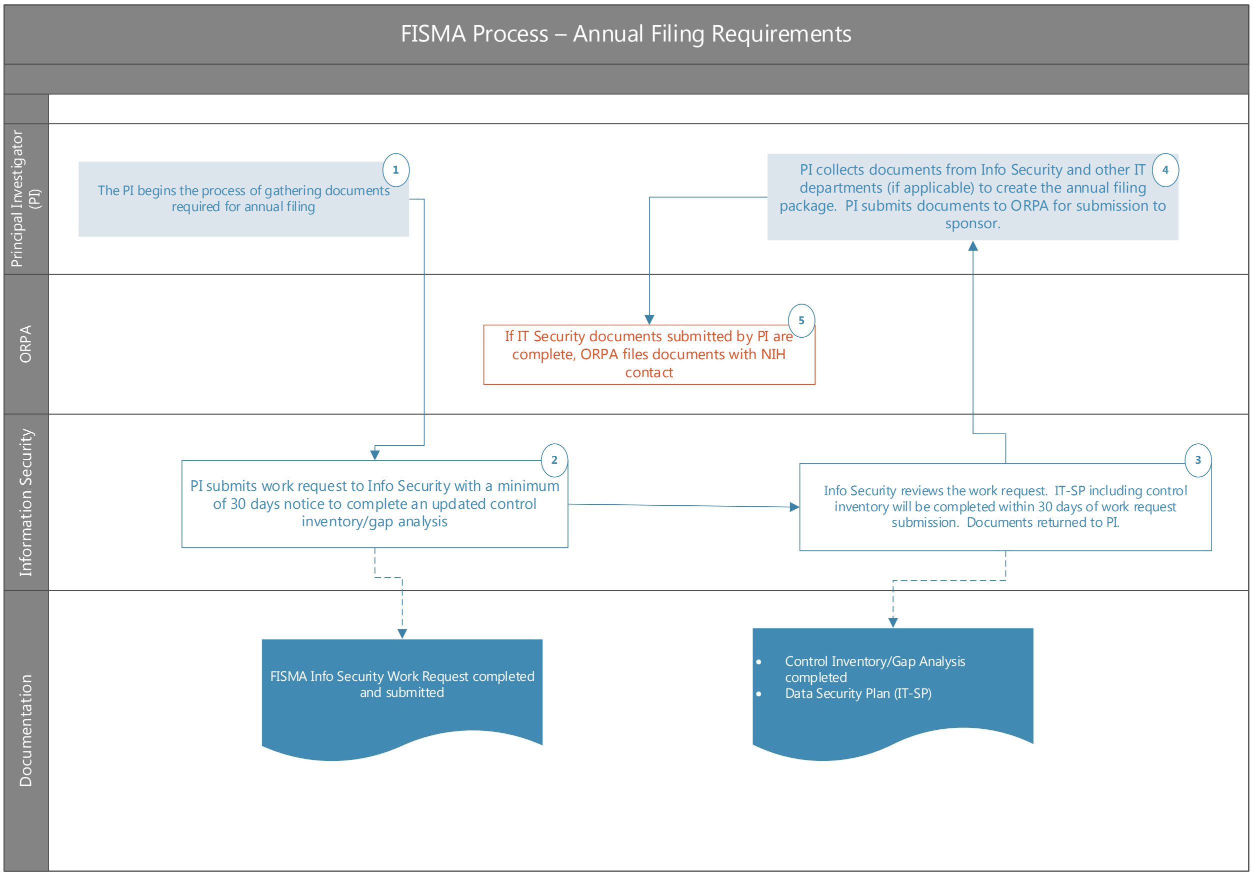
4 PI provides documents obtained from Info Security to ORPA for submission to sponsor. ORPA approval or additional guidance is provided to PI

5 Meeting scheduled with Info Security and PI to discuss list of controls required and expectations of PI

6 PI collects/maintains documentation from Info Security and IT (as needed). Information presented to ORPA for review

- FISMA Info Security Work Request completed and submitted
- PI presents list of identified controls
- Contract

- Risk Assessment
- Data Security Plan (IT-SP)
- Control Inventory/Gap Analysis



FISMA Process – Annual Filing Requirements
Principal Investigator (PI)
ORPA
Information Security
Documentation
1
2
3
4
5

1 The PI begins the process of gathering documents required for annual filing

2 PI submits work request to Info Security with a minimum of 30 days notice to complete an updated control inventory/gap analysis

3 Info Security reviews the work request. IT-SP including control inventory will be completed within 30 days of work request submission. Documents returned to PI.

4 PI collects documents from Info Security and other IT departments (if applicable) to create the annual filing package. PI submits documents to ORPA for submission to sponsor.

5 If IT Security documents submitted by PI are complete, ORPA files documents with NIH contact

FISMA Info Security Work Request completed and submitted

- Control Inventory/Gap Analysis completed
- Data Security Plan (IT-SP)