

University of Rochester & FISMA (Federal Information Security Management Act) Requirements

The Federal Information Security Management Act of 2002 (44 U.S.C. § 3541) is a United States federal law enacted as Title III of the E-Government Act of 2002 (P.L. 107-347, 116 Stat. 2899). 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*. This means that, under some Federal contracts or grants, information the University collects, or information systems the University uses to store research results will need to comply with FISMA.

To date, the University has accepted contracts with the National Institutes of Health (NIH) that require compliance with this Act. However, the regulatory environment is constantly changing, so all Request for Proposal (RFP), grant and contract language needs to be reviewed closely to identify FISMA or other information security requirements. It is important that researchers identify FISMA language in grant or contract proposals as soon as possible and alert the [Office of Research and Project Administration \(ORPA\)](#) and/or the [Office of Regulatory Support \(ORS\)](#) so that we can adequately respond to, and budget for, this complicated compliance requirement.

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 provide:

- Confidentiality - preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information;
- Integrity - guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity; and
- Availability - ensuring timely and reliable access to and use of information.

What do I need to do if I have a Request for Proposal, grant or contract that includes FISMA compliance language?

- Work with ORPA [and/or ORS](#) to identify how the federal agency has categorized the information and information systems you will have access to. Security categorization provides a structured way to determine the criticality and sensitivity of the information and

to assign a security impact value (low, moderate, high) for the security objectives of confidentiality, integrity, or availability. Has the sponsor clearly identified the information and information system classification (FIPS 199)?

- Once the overall security impact level of the information system is determined (after the system is categorized), an initial set of security controls is selected from the corresponding low, moderate, or high value. You will need to coordinate with ORPA, ORS and appropriate information technology resources (ISD for URMIC departments/staff; UIT for non-URMIC departments/staff) to identify and estimate the resources required to implement the required security controls and to manage the initial and ongoing roles and responsibilities for the Certification & Accreditation (C&A) process.

What are other considerations/questions that I need to consider? (ORPA, ORS and/or IT staff can assist you with these questions.)

1. Do you have detailed documentation of IT resources and support being provided by the sponsor?
2. Is a full **Certification & Accreditation (C&A)** required?
 - a) If yes, has the Certifying Authority (CA) been identified?
 - b) If no, is there text that clearly defines the scope of the requirements and the process for approval or certification?
3. Has the sponsor provided you with templates for any documentation?
4. Scope:
 - a) What non-UR systems (including network, servers, applications, databases & personal computing devices) and storage media will be used to create, access, transmit or receive data/records?
 - b) What UR-owned systems (including network, servers, applications, databases & personal computing devices) and storage media will be used to create, access, transmit or receive data/records?
5. Have you consulted with University HR as to any required back-ground checks for individuals involved in this research? Are there any requirements in addition to the University's current **Pre-employment Screening** criteria?
6. What internal resources will be required for FISMA compliance:
 - a) External consultants to manage the C&A requirements?

- b) IT support and coordination for FISMA compliance?
 - c) HR support and coordination for FISMA compliance?
7. Create a project charter:
- a) Define roles & responsibilities for Project Sponsor, Project Manager as well as technical, functional and deployment leads.

Estimate resources and estimated costs associated with each of those resources.

Necessary Resources for FISMA Compliance

- The documentation requirements as well as the administrative, technical and physical security controls are substantial. Resources required for FISMA compliance may require outside consultants. UR IT staff can identify consultants that have been approved by the University. The consultants will need to coordinate all C&A activities with the appropriate information technology resources (ISD for URM staff/departments; UIT for non-UR staff/departments).
 - Doing an initial risk assessment, determining the required resources (including funding), and determining how to integrate security controls into the existing UR infrastructure, requires substantial time and effort. Many of the costs associated with FISMA compliance may be project-specific and should be allocated to the proposal budget. Allot a substantial time-frame before proposal submission to coordinate with IT and other University departments to address these issues.
-