Federal Information Security Management Act of 2002 (FISMA)
Frequently Asked Questions*

What is FISMA?

FISMA is a certification granted by the US General Services Administration (GSA) that requires each *Federal Agency* to develop, document and implement an information security system for its data and infrastructure.

Why does OSU care about FISMA?

A 2010 Office of Management and Budget memorandum was issued requiring every Federal Agency to report their FISMA activities to Congress. The memo also reinforced the requirement that agencies include FISMA requirements in ALL contracts involving **sensitive data** as well as in grants where sensitive information is created, accessed, or stored of the Federal Government. Failure to comply with FISMA can result in contract termination by default and the loss of future contracts.

Does every contract require the same level of security?

The FISMA Certification and Accreditation process identified three security categories to identify systems: Low, Moderate, and High. Each level has a mandatory set of security controls and each level builds on the previous one. FISMA also mandates separate evaluations for the security for **confidentiality, integrity,** and **availability** of the sensitive data. The overall system level is the *highest* level for each of the three areas. The following example is provided as an illustration:

Research data containing individually identifiable health information would pose significant consequences if that data were stolen, lost, or accidentally disclosed making the confidentiality security category "Moderate." The data may not require 24 x 7 access so the security category for availability would be "Low." This might appear in a contract as:

Overall System Security Category	☐ Low ☒ Moderate ☐ High		
Overall Impact Levels (High Water Mark)	*Confidentiality*	*Integrity*	*Availability*
	Moderate	Low	Low

How do I know if FISMA is a requirement in my project?

Federal agencies have different ways of putting FISMA requirements into award documents. The most obvious would be by simply including a requirement for FISMA compliance in the Statement of Work (SOW). There would also probably be a requirement to submit a **System Security Plan** (SSP) and to obtain an "**Authority to Operate**" from the project sponsor. Other contracts might have articles or clauses called "Information Security;" may have a reference to comply with OMB A-130, FIPS 199, or similar language; or there may be language inserted into the contract requiring that the project "comply with all applicable NIST standards." The information could be included in the original contract but could also appear in modifications or renewals issued in 2010 or later.

I do have FISMA requirements for my project; how quickly can the process be completed?

The length of time to obtain FISMA compliance is highly variable and depends on factors including the security category (Low, Moderate, High), the availability of resources with skills and time to manage the process, current level of security controls, total number of users in a project, complexity of the computing environment. A small project, with few users, a mature control system and a Low security category could probably be done in a few months but a large project with a Moderate security category could take more than a year. It is unlikely that a project with a High security category could be undertaken at Oklahoma State University.

Who do I call for assistance with FISMA requirements?

Contact your college IT specialists for assistance. Keep in mind that it may take several months to become FISMA compliant so it is important to begin the process to meet FISMA (or other information/data security) requirements even before an award referencing the requirements is made. For administrative assistance with FISMA issues contact Toni Shaklee, Office of the Vice President for Research (toni.shaklee@okstate.edu or 42361).

*Adapted from: FISMA FAQs produced by the Health Affairs Information Systems, University of California-Irvine (Version 1.1, April 11, 2012)