**Federal Information Security Management Act (FISMA)**

**Background**

The Federal Information Security Management Act, or FISMA, is a federal law enacted in 2002. FISMA provides the framework for the creation of standards related to federal information systems. FISMA requires each federal agency to develop, document and implement an agency-wide program to provide information security for information and information systems that support the operations and assets of the agency, including those provided or managed by another agency or contractor.

FISMA standards were developed and published by the National Institute of Standards and Technology (NIST). NIST has published several documents related to the standards that are applicable both to federal agencies and to contractors (like ISU) that may be required to comply with the standards when providing services.

The standards provide for security categorization levels that indicate the type of security requirements necessary to protect the IT system or data. Categories include confidentiality level; integrity level; availability level; and overall level. The levels include Low, Moderate and High.

Federal agencies have begun to flow down the requirements of FISMA in contracts, cooperative agreements, and even in grants. At ISU, OSPA has identified FISMA terms and conditions in agreements from the US Department of Agriculture, the US Department of Transportation, the US Department of Defense, and the Iowa Department of Public Health. These agreement terms may or may not indicate the FISMA security category and level applicable to the work proposed under the award. These terms may or may not be applicable to your project.

**When Would FISMA Apply to Your Sponsored Project?**

FISMA may apply to your sponsored project when your project involves collecting, storing, processing, transmitting or using information **on behalf of** a federal agency. The phrase “**on behalf of**” is not defined in the law; however, “on behalf of” could be interpreted as applying to those projects for which ISU acts as a direct extension of a federal agency or when ISU may be accomplishing a federal government function for a federal agency. Additionally, FISMA could apply to your project if you will be transmitting data to a federal system or if you need to utilize or access a federal system for the scope of work.

**FISMA – Budgeting for a Sponsored Project**

Compliance with the requirements of FISMA may be costly. Researchers need to be aware of the FISMA security category and level required in an award in order to make an assessment of potential cost. Researchers should consult with ISU Information Technology Services (ITS) to develop a “buy vs. build” analysis to develop an appropriate cost estimate for FISMA compliance. Note that ISU IT systems are not compliant as a whole with FISMA and creating FISMA compliant systems within ISU will incur costs that should be budgeted in your sponsored project budget. However, it may not be possible to configure ISU IT systems to conform to FISMA requirements for any particular project. As a result, researchers may need to consider the hire of a third party IT systems contractor that is FISMA compliant to provide FISMA related services and include these costs in the proposal budget. Researchers may contact OSPA, OIPTT or ITS if they have questions regarding FISMA compliance. See contact information listed below.

**FISMA award terms**

Federal awards may contain references to FISMA that are labeled in various ways. You may see references to NIST, system security plan requirements, information security assessments or document references such as 800-53. Typically, federal contracts with FISMA requirements will have a section of the agreement entitled “Information Security”; grants or cooperative agreements may have a section entitled “FISMA compliance.” OSPA will review agreements for FISMA clauses and will work with the researcher and the agency to determine whether the clause applies to the work being conducted under the award. If the clause does not apply, OSPA will request the agency provide a written determination of non-applicability. If the clause does apply, the researcher should work with ISU ITS to discuss IT system requirements and cost, if the cost of compliance was not included in the award budget. It may be necessary for ISU to request additional funds from the agency to comply with FISMA requirements if the cost has not been included in the original budget request.

**FISMA Information**

More information on FISMA may be found at:

NIST FISMA URL: <http://csrc.nist.gov/groups/SMA/fisma/index.html>

**OSPA/OIPTT Contact Information**

To discuss FISMA requirements at the time of proposal submission, please contact the OSPA PreAward Team at ospa-proposals@iastate.edu. To discuss FISMA agreement terms and conditions at the time of award, please contact ospa-awards@iastate.edu or industry-contracts@iastate.edu (for industry and commodity awards).

**ITS Contact Information**

To discuss development of a buy vs. build analysis for FISMA compliance and/or obtain interpretation assistance on the security and technology implications of FISMA requirements, please contact the ITS Director of Security Operations, Andrew Albinger at albinger@iastate.edu or 294-3984.