**Data Security: FISMA**

**What are the key acronyms I need to know?**

* FISMA:  Federal Information Security Management Act of 2002
* NIST:  National Institute of Standards and Technology
* CUI:  Controlled Unclassified Information

**What is FISMA?**

* FISMA is a law which provides protection for federal information systems against natural, man-made, or system-generated threats
* FISMA is different from standard data security controls in that it requires additional controls for which we have a specialized environment.
* Each federal agency, vendor, or contractor must develop, document, and implement an institution-wide program to provide information security for the information systems that support the operations and assets of the institution, contractors, or other sources.
* NIST provides guidance for FISMA compliance via its Special Publications (SP) 800 series.

**I am considering a project or contract which has FISMA requirements. Where do I start?**

* Notify the Office of Sponsored Programs and the FISMA Program Manager, Eric Asare.
* Review the FISMA Compliance: Principal Investigator’s Requirements document.
* Review the [FISMA Information Sheet](https://ctsi.wakehealth.edu/-/media/WakeForest/CTSI/Files/Regulatory/Data-Security/FISMA-Information-Sheet-FINAL.docx)for commonly required information.  The FISMA Program Manager will work with the PI and the Study Team to clarify information needed and assist with completing the FISMA assessment process.

**What are the benefits to WFBMC of being FISMA compliant?**

* Being FISMA compliant enables WFBMC to compete for certain research grants and contracts.
* FISMA compliance reduces the risk of research data breaches.
* FISMA compliance can potentially save WFBMC from incurring substantial fines and financial loss due to privacy breaches and misuse of stolen sensitive information

**What are the risks of non-compliance?**

* All projects with federal funding components MUST comply with all applicable federal regulations.  Failure to comply can affect current and future funding from federal agencies.
* Non-compliance can affect the reputation of the Institution and its affiliate institutions or influence other institutions’ interest in collaborating with us on a grant or sub-contract.
* The Institution, faculty, and staff may be subject to corrective actions, including fines and penalties, according to the required Federal and Institutional policies.

**What are the key steps in the FISMA assessment process?**

* Categorize information and information systems according to risk level. Risk Levels are defined below.
* Maintain a system security plan
* Utilize security controls appropriate for the risk level.  FISMA Security Controls are outlined below.
* Conduct risk assessments throughout the life cycle of the system
* Institute certification and accreditation of the systems, including staff, processes, and technology
* Conduct continuous monitoring of the authorized system

**How are FISMA requirements different from our general data security requirements?**

* FISMA builds upon existing institutional security requirements such as password policies, firewalls. Privacy/confidentiality, data integrity and business continuity.
* FISMA imposes additional security requirements consistent with the level of risk of the data.

**Which funders and grant mechanisms are most likely to have FISMA requirements?**

* National Institutes of Health (NIH)
* Centers for Disease Control (CDC)
* Department of Defense (DoD)
* Veterans Administration (VA)
* National Aeronautics and Space Administration (NASA)
* National Oceanic and Atmospheric Administration (NOAA)
* Other governmental Agencies

**How do I determine if FISMA is required of my project?**

* Review grant or contract applications to determine if there are FISMA requirements. Look for terminology related to FISMA deliverables such as:
* System Security Plan (SSP)
* Risk Assessment Report (RAR)
* Authorization to Operate (ATO)
* Review our [FISMA deliverables document](https://ctsi.wakehealth.edu/-/media/WakeForest/CTSI/Files/Regulatory/Data-Security/FISMA-Deliverables-FINAL.docx).

**What are the FISMA risk levels?**

* The risk level categorization is based on the critical level of the information system/type according to each of the three security objectives: Confidentiality, Integrity and Availability (CIA). The higher the risk level, the more controls apply to the project.
* **Low** – if data is already publicly available and the data will have limited impact to the government and national economy if the data were breached
* **Moderate**– if the data will have a serious impact when breached or compromised; includes PHI
* **High** – if the data would have a severe impact on government systems and operations and may even lead to financial ruin or economic crisis if breached or compromised;

**What are FISMA controls?**

* There are over 800 security controls organized into 16 families.  Controls are either technical, operational, or management in nature. Depending on the level of risk, certain controls must be in place.  Some controls are already in existence with our general Information Technology Security Systems.   However, additional controls may be indicated.
* Sixteen Security Control Families
* Risk Assessment
* Certification, Accreditation and Security Assessments
* System Services and Acquisition
* Security Planning
* Configuration Management
* System and Communications Protection
* Personnel Security
* Awareness and Training
* Physical and Environmental Protection
* Media Protection
* Contingency Planning
* System and Information Integrity
* Incident Response
* Identification and Authentication
* Access Control
* Accountability and Audit

**What is involved in WFBMC’s FISMA compliance review process for an individual project/contract?**

* The institution must complete a Security Assessment and Authorization (SA&A) review for your project to determine compliance with requirements consistent with the security level.
* The PI will complete the FISMA Information Sheet [ADD LINK] and send this to the FISMA Program Manager.
* The PI and study team will collaborate with the FISMA Program Manager to:
* Determine the scope of FISMA compliance;
* Complete the Security Controls Assessment;
* Implement any additional needed controls; and
* Prepare required FISMA deliverables.
* Most contracts dictate a timeline of when deliverables are due. The FISMA Program Manager will assist the PI and study team to prepare the required deliverables.  Below are *examples* of Department of Health and Human Services (DHHS) contract specifications:
* IT Security Plan - due within 30 days after contract award (same as System Security Plan above)
* IT Risk Assessment (IT-RA) - due within 30 days after contract award
* FIPS 199 Standards for Security Categorization of Federal Information and Information Systems Assessment (FIPS 199 Assessment) - due within 30 days after contract award.
* IT Security Assessment and Authorization (IT-SA&A) - due within 3 months after contract award
* See “FISMA Deliverables” for more information and sample documents of selected deliverables.

**How long will it take to assure that the security for my project is FISMA compliant?**

* On average it may take six months to complete the Security Assessment and Authorization (SA&A) process.
* The time it takes for a system to be in compliance depends on several variable factors such as system size, skilled human resources available, the complexity of the computing environment, software and hardware availability etc.
* All security does not have to be in place at the time of grant/contract submission or award.  The Notice of Award and/or contract typically outline the required deliverable due dates. Deliverable dates are determined as part of the assessment, indicating at what point different security measures must be implemented.  The institution must assure that the risk level is reasonable until all measures are in place.
* To meet FISMA deliverable deadlines, we strongly encourage you to contact the Office of Sponsored Programs and the FISMA program manager as soon as possible.
* Upon assurance that FISMA Requirements have been met, an Authorization to Operate (ATO) will be issued by WFBMC designated executive(s).  ATOs are valid for three years.

**What is required to maintain FISMA Compliance?**

* Compliance of all authorized systems with FISMA requirements must be monitored throughout the life of the project and until all data has been analyzed.
* An Authorization to Operation (ATO) is valid for 3 years.
* All FISMA assessments related to a project are subject to yearly renewal except Privacy Impact Assessments (PIA) which must be renewed every 3 years.
* The FISMA Program Manager will assist PIs and study teams in monitoring and maintaining FISMA compliance.

**We already have a grant project in progress, do I have a FISMA requirement?**

* Work with the Office of Sponsored Programs to determine if Notice of Award, contracts, etc. have FISMA requirements that must be addressed. If so, the Security Assessment & Authorization (SA&A) process must be completed or updated.

**How will FISMA impact the use of my data?**

* How do I use my data in compliant areas?
* There are no restrictions on the proper use of data from FISMA point of view (as long as it falls within the scope of your research)
* If electronic data will need to be shared with other individuals or institution, it may be necessary to establish an Interconnected System Agreement and Memorandum of Understanding
* As a PI, do I have to keep records? Submit reports outside?
* Copies of deliverable will be given to the PI for record. OSP will liaise with Federal agencies on issues of FISMA Compliance

**What are we doing at the institutional level to comply with FISMA requirements?**

* A FIMSA Compliance Committee has been established with representatives from IT, CTSI, and other research stakeholders to address institutional needs related to FISMA.
* Options are being investigated for storage of FISMA-related data in a separate, even more secure environment, consistent with FISMA requirements.
* A FISMA Program Office has been created to facilitate the processes and procedures involved to support compliance.
* The following Information Technology security [policies](https://intranet.wakehealth.edu/my.policy) related to FISMA; others are under development:
* Risk Management Policy
* System and Services Acquisition Policy
* Configuration Management Policy
* System and Communications Protection Policy
* Personnel Security Policy
* Awareness and Training Policy
* Physical and Environmental Protection Policy
* Media Protection Policy
* Contingency Planning Policy
* System and Information Integrity Polic
* Incident Response Policy
* Identification and Authentication Policy
* Access Control Policy
* Accountability and Audit Policy

* General boilerplate language for Information Technology Services and the Federal Information Security Modernization Act can be found at CTSI’s Boilerplate collection at CTSI.wakehealth.edu.  This may be sufficient to include in a grant application.  The FISMA Program Manager can assist in providing more detailed information as needed.

**What resources are available to assist me/my team with FISMA related questions?**

* + Consultation and assistance are available for reviewing grant proposals, contracts, and notices of award for FISMA requirements: contact CTSI Office of Sponsored Programs, Ryan Favreau at 336-713-5306.
	+ Consultation and assistance are also available for conducting risk assessments, and training for PIs and study teams. Contact IT Security at 336-713-ITSO (3-4876) or ITsecurity\_dl@wakehealth.edu or privacy@wakehealth.edu for assistance.

**Forms and Templates**

* [FISMA Principal Investigator Requirements (.pptx)](https://ctsi.wakehealth.edu/-/media/WakeForest/CTSI/Files/Regulatory/Data-Security/FISMA-Principal-Investigator-Requirements.pptx)
* [FISMA Deliverables (.docx)](https://ctsi.wakehealth.edu/-/media/WakeForest/CTSI/Files/Regulatory/Data-Security/FISMA-Deliverables-FINAL.docx)
* [FISMA Information Sheet (.docx)](https://ctsi.wakehealth.edu/-/media/WakeForest/CTSI/Files/Regulatory/Data-Security/FISMA-Information-Sheet-FINAL.docx)