NCI Cyber Governance and Compliance

*SEER*DMS*

NIH NATIONAL CANCER INSTITUTE

September 26, 2018

Version 09_26_18

Agenda

- *Who Are We and How Can We Help?*
- *What is FISMA?*
- *What is The Risk Management Framework?*
- *When Does FISMA apply?*
- *FISMA Systems Categorization*
- *Thoroughness of FISMA Areas of Evaluation*
- *FISMA Package Requirements*
- *FISMA Benefits*
- *NCI's Cyber Partnership With The Research Community*

Who are We and How Can We Help?

- NCI Cyber Governance and Compliance Team (GCT)
  - Responsible for the cyber governance and compliance oversight of all NCI internal, contractor-hosted, and cloud hosted federal systems
    - Craig Hayn
    - Eric Scott
    - Dale Lamb
- We are the eyes and ears of the NCI Information Systems Security Officer (ISSO) – Bruce Woodcock
- We assist business and system owners with:
  - Providing FISMA/RMF Guidance
  - Security policy analysis and interpretation
  - Risk Analysis and Risk Management (we advise the ISSO and CIO)
  - FISMA documentation review (IV&V)
  - Answering Questions
  - Providing Templates

What is FISMA?

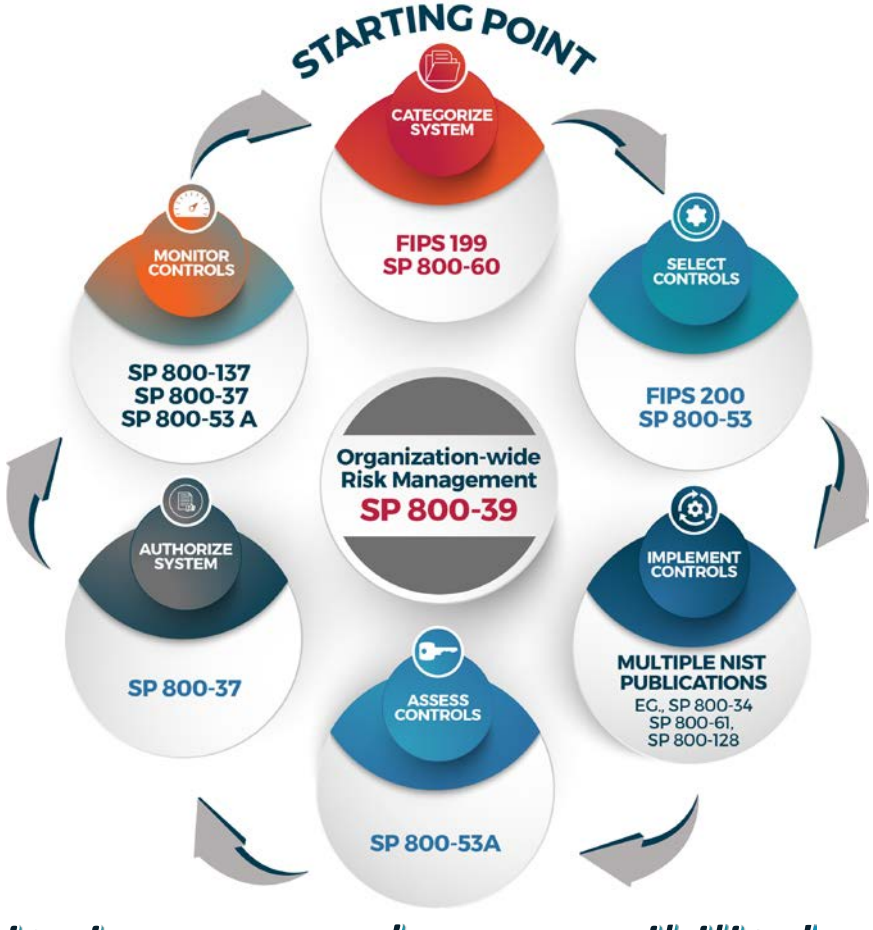
- Federal Information Security Management Act
  - a federal law passed in 2002 as part of the e-Government Act that requires federal agencies to develop, document, and implement an information security and protection program
  - Mandated that all federal information systems be authorized to operate (in writing) by a government risk executive
- FISMA was updated in 2014 and is now called the Federal Information Security Modernization Act of 2014
  - Updated law emphasizes cybersecurity continuous monitoring, risk management, and incident response
  - Requires security assessment and authorization (SA&A) of all federal information systems using the risk management framework (RMF)
- Requires auditing and quarterly and annual reporting to Congress
- **All Federal Information Systems must comply with FISMA and have an authorization to operate (ATO)**

What is the Risk Management Framework or “RMF”?

- Common information security framework to facilitate the FISMA requirements

- Six-step lifecycle designed to build information security capabilities into information systems through the application management, operational, and technical security controls.
  1. Categorize
  2. Select
  3. Implement
  4. Assess
  5. Authorize
  6. Monitor

- Developed and maintained by the National Institute of Standards and Technology (NIST)



Security is everyone’s responsibility!

When does FISMA Apply?

- FISMA applies to all internal, contractor-hosted, and cloud hosted federal information systems
  - An information system is defined as a *discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of federal information*.
- How does the government determine if a system is Federal or non-Federal in nature?
  - We primarily examine the contract language as well as data ownership
  - If the government directs the contractor to collect, store, or process data on its behalf, or if the information is "owned" by the government, it usually means the system will be a government system.
  - Exceptions are considered and made on a case-by-case basis. The SEER DMS has both federal and non-federal components.

  - **For the purposes of SEER*DMS, the individual Registries are not considered federal systems, but IMS/DMS is a Federal system and is going through robust efforts to ensure your data is protected.**
    - FISMA does not apply to the Registries because the states would collect the data with or without federal support, and the Registries "own" their data.
    - Once the data is shared with the government (i.e., through our contract with IMS), the government becomes a custodian of the data and is obligated to treat it as a federal system while in our control; thus, the IMS DMS is going through FISMA SA&A.

When FISMA Applies, How Are Systems Categorized?

- FISMA systems are assessed based on their security impact rating of Low, Moderate, or High
  - Impact ratings are established by considering the confidentiality, integrity, and availability (CIA) needs, using NIST-provided ratings guidance (FIPS-199 and NIST 800-60)
  - Systems must be assessed by a qualified assessor and without causing conflict of interest
  - The NCI GCT ensures assessors are qualified before allowing assessment to be conducted
    - Moderate and High impact systems must be assessed by an independent assessor. If you are ever unsure, please check with the NCI GCT.
- FISMA systems are further grouped into functional categories based on operational factors:
  - General Support System (GSS) (*interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people*)
  - Major Application *(information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources)*
  - Minor Applications *(An application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a general support system)*

FISMA Ensures a Thorough Review of Security and Privacy Related Controls

SA&A process fulfills the FISMA requirements through the RMF and includes:

- Access Control
- Audit and Accountability
- Awareness and Training
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical and Environmental Protection
- Planning
- Risk Assessment
- Program Management
- Security Assessment and Authorization
- System and Communications Protection
- System and Information Integrity
- System and Services Acquisition
- Privacy: Authority and Purpose
- Privacy: Accountability, Audit, and Risk Management
- Privacy: Data Integrity
- Privacy: Data Minimization and Retention
- Privacy: Individual Participation and Redress
- Privacy: Security
- Privacy: Transparency
- Privacy: Use Limitation

The FISMA Authorization Package Requires Multiple Artifacts

A full SA&A package may require any or all of these artifacts:

- ❑ FIPS-199 System Categorization
- ❑ E-Authentication Threshold or Risk Analysis (eTA/eRA)
- ❑ Business Impact Analysis (BIA)
- ❑ System Security Plan (SSP)
- ❑ Privacy Impact Assessment (PIA)
- ❑ Interconnection Agreements (e.g., ISA and/or MOUs), if applicable
- ❑ Configuration Management Plan (CMP)
- ❑ Contingency Plan (CP)
- ❑ Contingency Plan Exercise Report (if Moderate impact FIPS rated, then a live exercise is required)
- ❑ Security Assessment Plan (SAP)
- ❑ Security Assessment Report (SAR)
- ❑ Plan of Action and Milestones (POA&M)
- ❑ ATO Letter signed by Federal Authorizing Official (AO)

For additional NIH specific guidance reference NCI's FISMA Process Guidance and Templates:

https://cbiit.cancer.gov/contractor-security-guidance

What Are Some of FISMA's Benefits?

- Helps ensure your systems' Confidentiality, Integrity and Availability (C-I-A) are protected
- Provides standardized approach for selecting security controls based on a system's risk rating (i.e., Low, Moderate, or High risk baselines)
- Enables security integration throughout the system's lifecycle by informing design and modification decisions
- Makes security more cost-effective when applied throughout the lifecycle, rather than when retrofitted
- Helps system owners and risk executives better assess security controls' effectiveness
- Enables organizational risk executives to make better and more credible authorization decisions
- Allows agencies to articulate and understand system interconnection and data sharing risks
- Lowers risk to the agency, its operations, data, constituents, and other stakeholders who entrust us with their data – like our SEER*DMS partners

Remember, Security is EVERYONE'S responsibility!

How Does NCI Partner With The Research Community?

- NCI maintains research partnerships across:
  - Industry
  - Academia
  - Laboratories
  - Other Institutes and Centers
- The NCI GCT works with all entities to ensure a smooth and successful FISMA implementation and compliance
- We work with partners to ensure they achieve and maintain their compliance posture by following NIST and Agency-required Continuous Monitoring and Risk Management activities
- In the case of SEER*DMS, the NCI Governance and Compliance Team has a strong relationship with the IMS/DMS Team, and we have worked closely with IMS for over 12 years
  - NCI and IMS will use FISMA RMF to ensure that your data are properly and adequately protected while in our custody
  - NCI works closely with IMS as the systems integrator and data custodian.
    - IMS Chief Technology Officer, Scott Depuy