Applying FISMA & NIST to Academic Research

Executive Summary

Many academic institutions with large research portfolios receive more than half of annual research revenue from federal sponsors. The federal government invests over $100 billion in research and development programs each year. The information age yields exponential growth and truly innovative advances in science and data, but with it comes the great responsibility to address privacy and security. Information security programs are commonplace for most organizations in the 21st century, and just as organizations protect key business infrastructure, they must also secure and protect federally regulated data used in the name of research.

Protecting research information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction is a critical component to safeguarding research information and preventing financial loss or damage to the university's reputation. Protecting confidential information is not only a legal and business requirement, but is also an ethical requirement.

Due to increased cybersecurity concerns throughout the world, research sponsors are including more stringent requirements for working with restricted data. There is a notable increase in the number of grants and contracts requiring the university to implement specific privacy and security safeguards for data and information systems as mandated by federal (HIPAA, FISMA, NIST, FERPA, GLBA, ITAR, Privacy Act), state and/or local law, industry sanctioned (PCI-DSS), university policies (i.e. UF Privacy Office, Security Office) or agreements (i.e. Data Use Agreement, Business Associate Agreement, etc.).

Over the past eight months, several University of Florida (UF) offices partnered to design and implement Research Shield (ResShield), a computing environment hosted by UF Information Technology (UFIT) for use by researchers who are working with regulated data. The driving force behind this strategic initiative is a $40M contract between the UF on behalf of its Institute for Child Health Policy (ICHP) and the Texas Health and Human Services Commission (HHSC). In 2014, Texas HHSC inserted FISMA compliance in the contract terms and conditions.

The current ResShield architecture is designed to meet moderate level security and privacy controls as specified in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53_Rev4. Approximately 267 controls are in place across the 18 control families defined by NIST.

Further analysis of UF's research portfolio revealed the need to accommodate varying levels of information security requirements. In partnership with the Office of Research, UFIT is expanding the ResShield architecture to support a comprehensive information security program for academic research. Driving principles for the expansion include:

1. Incorporating economic models to determine the optimal amount to invest for protecting a given set of information (see NIST SP 800-65 or Gordon-Loeb Model)
2. Designing system architecture to support varying degrees of security and privacy controls (i.e. HIPAA, Controlled Technical Information, Controlled Unclassified Information, NIST Low, NIST Moderate, NIST High)

Protecting research information without compromising response time, business agility and competitive advantage is of the utmost importance for continued growth in research portfolios. This infrastructure also has the potential to accelerate scientific discoveries by enabling faster, more secure access to data. The infrastructure to support these critical needs must be cost-efficient with a sustainable funding model.

This white paper is intended to provide an overview of the method the University of Florida used to implement the NIST Risk Management Framework and create an information security program for academic research. It may serve as a guideline to help other institutions implement such a framework. Understanding the institution's research landscape is key for designing a cost-effective infrastructure that yields the return on IT investment.

Contents

Executive Summary 1
FISMA vs NIST 3
What is FISMA? 3
What is NIST? 3
NIST Risk Management Framework 4
Diagram 1: NIST RMF 4
Table 1: 6-Step NIST RMF with Supporting Publications and Guidance 4
Applying NIST RMF to Academic Research 5
Step 1: Categorize 5
Table 2: NIST Publications for Step 1 – Security Categorization 5
Table 4: Sample Documentation for NIST RMF Security Categorization 7
Step 2: Select Security Controls 8
Table 5: NIST Publications for Step 2 – Select Controls 8
Table 6: Number of NIST Security Controls by Family (Total and Minimum Number per Security Categorization) 8
Contributors from the University of Florida 10
Executive Sponsors 10
UF Implementation Team 10
Appendix A: Federal Information Types and NIST Impact Ratings 11
Mission Based Information Types (94 total) 11
Management and Support Information Types (77 total) 14

FISMA vs NIST

What is FISMA[1]?

The Federal Information Security Management Act (FISMA) is a United States (US) federal law enacted as Title III of the 2002 E-Government Act (Pub.L. 107–347, 116 Stat. 2899). FISMA requires federal agencies, and those providing services on their behalf, to develop, document, and implement security programs for information systems. The act recognized the importance of information security to US economic and national security interests. FISMA brought attention to cybersecurity within the federal government and explicitly emphasized a "risk-based policy for cost-effective security".

In April 2010, the Office of Management and Budget (OMB) issued a memorandum requiring all federal agencies to report their FISMA activities to Congress. FISMA requires federal agency program officials, chief information officers, and inspector generals (IGs) to conduct annual reviews of the agency's information security program and report the results to the OMB. OMB uses these data to assist in its oversight responsibilities and to prepare the annual report to Congress on agency compliance with the act.

The 2010 OMB memo also reiterated the requirement for federal agencies to include FISMA compliance in all contracts involving federally regulated data, as well as grants where regulated data are created, accessed, or stored on behalf of the federal government. While FISMA generally applies to federal agencies, FISMA compliance is increasing for recipients of federal grants and contracts.

What is NIST[2]?

Founded in 1901, the National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the US Department of Commerce. NIST's mission is to promote US innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways to enhance economic security and improve our quality of life.

FISMA gives NIST statutory responsibilities to establish non-product specific guidelines and standards to ensure a reasonable level of security in government systems. Balancing organizational risk with cost-efficient strategies is the foundation for developing an effective information security program.

As a key element of the FISMA Implementation Project, NIST developed an integrated Risk Management Framework (RMF) to promote the development of comprehensive and balanced information security programs. The term "FISMA compliance" is often used to describe the process organizations go through to implement the NIST RMF and related standards and guidelines. The RMF emphasizes:

- Building information security capabilities into federal information systems through the application of state-of-the-practice management, operational, and technical security controls;
- Maintaining awareness of information system security though ongoing and enhanced monitoring processes;
- Providing essential information to senior leaders to facilitate decisions regarding the acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation arising from the operation and use of information systems.

NIST standards and guidelines, including the RMF, are categorized in the following types of publications:

1. Federal Information Processing Standards (FIPS)
2. Special Publications (SP)
    a. SP 800-series – Computer Security
    b. SP 1800-series – Cybersecurity Practice Guides
    c. SP 500-series – Computer Systems Technology
3. NIST Internal/Interagency Reports (NISTIR)
4. Information Technology Laboratory Bulletins (ITL Bulletins)

[1] Federal Information Security Management Act of 2002. (n.d.). In Wikipedia. Retrieved November 25, 2015, from https://en.wikipedia.org/wiki/Federal_Information_Security_Management_Act_of_2002

[2] NIST General Information. (n.d). Retrieved November 25, 2015, from http://www.nist.gov/public_affairs/general_information.cfm

NIST Risk Management Framework

The NIST Risk Management Framework (RMF) includes six steps to guide organizations through the process of assessing risk and then selecting the appropriate controls to secure information systems. The steps and corresponding NIST publications are visualized in Diagram 1 and defined in Table 1:

Diagram 1: NIST RMF

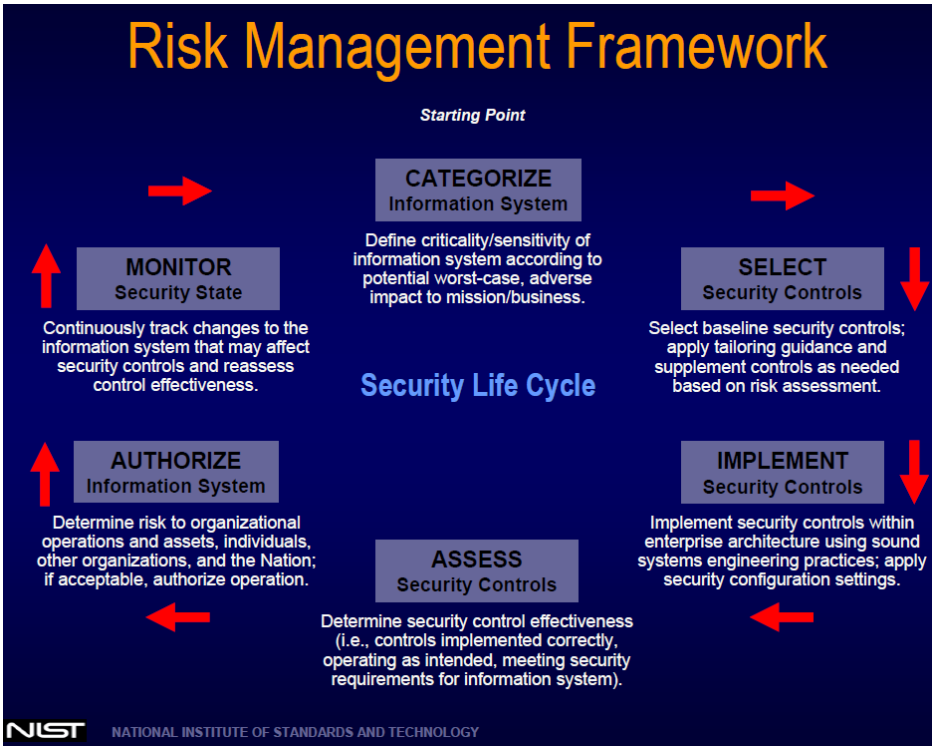


Table 1: 6-Step NIST RMF with Supporting Publications and Guidance

Steps 1 - 6	Description	NIST Publications	Additional Guidance
1. Categorize	Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business	FIPS199 SP 800-60 vol1 SP 800-60 vol2	FAQs Roles & Responsibilities Quick Start Guides
2. Select	Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment	FIPS200 SP 800-53	FAQs Roles & Responsibilities Quick Start Guides
3. Implement	Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings	SP 800-70	(not available yet)
4. Assess	Determine security control effectiveness (i.e. controls implemented correctly, operating as intended, meeting security requirements for information systems)	SP 800-53A	SP 800-53A: -XML -Assessment Cases
5. Authorize	Determine risk to organizational operations and assets, individuals, or other organizations, and the Nation; if acceptable, authorize operation of the information system	SP 800-37	Supplemental Guidance
6. Monitor	Continuously track changes to the information system that may affect security controls and reassess control effectiveness on a regular basis	SP 800-37 SP 800-53A	FAQs Roles & Responsibilities Quick Start Guides

Applying NIST RMF to Academic Research

The first step of the RMF results in a security categorization for the system. This categorization defines the remaining implementation work. It is important to note that federal agencies are responsible for determining the security categorization of federal information systems. If the information security categorization is unspecified in federal contract terms and conditions, the academic institution can apply the NIST RMF, including security categorization, to determine how best to proceed.

For academic institutions that choose to implement the NIST RMF, input from several stakeholders is required to successfully complete the first two steps in the NIST RMF. Key stakeholders include the Principal Investigator, Office of Research, Privacy Office, Information Security Office and other applicable IT departments. As part of a FISMA implementation, academic institutions should define core office roles and responsibilities. Once roles are defined, it is equally important to diagram a cross-functional flowchart outlining the institution's business process for identifying research projects that use regulated data and then assessing and managing risk associated with those data. Information security programs for academic research should address two critical factors:

3. Incorporate economic models to determine the optimal amount to invest for protecting a given set of information (see NIST SP 800-65 or Gordon-Loeb Model)
4. Design system architecture to support varying degrees of security and privacy controls (i.e. HIPAA, Controlled Technical Information, Controlled Unclassified Information, NIST Low, NIST Moderate, NIST High)

The remaining sections of this document focus on the first two steps in the NIST RMF (1-categorirze, 2-select), which require collaboration across several core offices in academic institutions. The last four steps in the NIST RMF (3-implement, 4-assess, 5-authorize, 6-monitor) guide the remaining work to implement, document and monitor the controls, and work for these steps is managed primarily by the IT departments.

Step 1: Categorize

In order to determine the security categorization of an information system, metadata (i.e. variables or field names) are analyzed with respect to three security objectives: confidentiality, integrity, and availability (C-I-A). When federal law or contract/grant terms and conditions require FISMA or NIST compliance, the security categorization is often applied to individual datasets rather than entire information systems. Although the analysis requires inspection of all data contents, the end result of step 1 is a single impact rating of low, moderate, or high (L-M-H) for the dataset or information system in question. Table 2 summarizes the NIST publications that guide the security categorization:

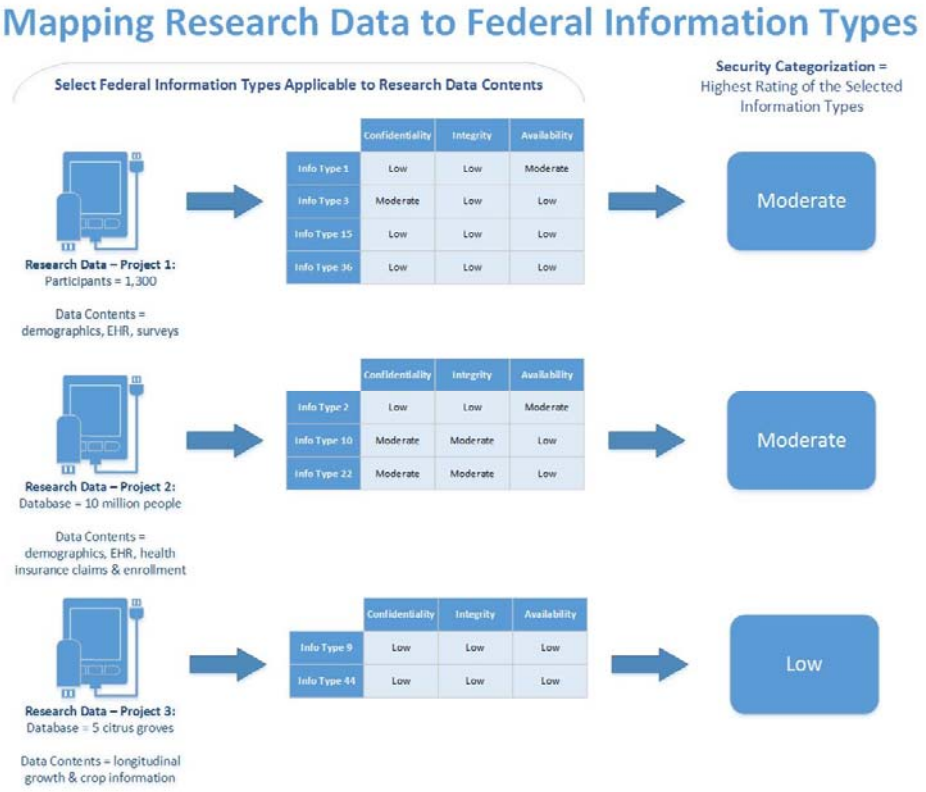
Table 2: NIST Publications for Step 1 – Security Categorization

NIST Publication Number	NIST Publication Title	Key Points
FIPS199 (13 pages)	Standards for Security Categorization of Federal Information and Information Systems	-Defines three security objectives (C-I-A) -Defines three impact levels (L-M-H) -Instructions on documenting security objectives and impact levels for information types and information systems
SP 800-60 vol1 (53 pages)	Guide for Mapping Types of Information and Information Systems to Security Categories	-Section 3 recaps FIPS199 -Section 4 details the step-by-step process for metadata analysis that leads to the single impact rating/security categorization
SP 800-60 vol2 (304 pages)	Appendices	171 federal information types and the corresponding NIST impact ratings for C-I-A are indexed in two categories. These appendices are used as part of the step-by-step process defined in section 4 of SP 800-60 volume 1: • App C: Management and Support (77 info types) • App D: Mission Based (94 info types)

FIPS199 and section 3 of SP 800-60, volume 1, defines the following matrix for analyzing information systems (or research project data) to determine potential impact associated with three primary security objectives:

Security Objective	Potential Impact		
	LOW	MODERATE	HIGH
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

NIST SP 800-60, volume 2, defines 171 specific information types, each with its own impact rating (L-M-H) for the three security objectives (C-I-A). See Appendix A of this document for a table summary of the information types and NIST recommended impact ratings. Understanding how research data contents map onto the NIST information types is key for assessing risk to the organization. In collaboration with the Principal Investigator, the Office of Research and applicable IT departments, research project data are mapped to federal information types, and the end result is the security categorization, as depicted in Diagram 2:



While NIST provides a comprehensive list of federal information types, it may be incomplete with respect to academic research data. It is important to note that, when applicable, NIST recommends adjustments to the list of information types or the corresponding impact ratings. Adding or revising information types based on the dataset or information system in question is allowed. In addition to revising information types, the NIST recommended impact ratings may also be adjusted.

Adjustments require proper justification, which must be documented as part of the implementation. Section 4.5 of NIST SP 800-60, volume 1, includes a suggested format for documenting the security categorization process. An example is provided in Table 4 below:

Table 4: Sample Documentation for NIST RMF Security Categorization

Information System Name: PCORI Project 00110492 (PI: Carden)			
The objective of this project is to determine the effect of an ED-to-Home Transitional Care Intervention on patients' self-reported quality of life and need for resource intensive, hospital-based care.			
Information Types			
D.14.1 Access to Care	The Health Care Coach is employed by the area Agency for Aging and works with the patient to navigate from the ER department back to their primary care provider.		
D.14.5 Health Care Research and Practitioner Education	This is an IRB approved research study to analyze Medicare claims and patient data with intervention data.		
D.20.1 Research and Development	Researchers will use secondary and primary datasets to understand the intervention effect on complex populations.		
Step 1: Identify Information Types	Step 2 [Provisional] / Step 3a [Adjustments]		
	Confidentiality Impact	Integrity Impact	Availability Impact
	Step 3b [Impact Adjustment Justification if applicable]		
D.14.1 Access to Care	L	M	L
	No adjustments	No adjustments	No adjustments
D.14.5 Health Care Research and Practitioner Education	L	M	L
	No adjustments	No adjustments	No adjustments
D.20.1 Research and Development	L	M	L
	No adjustments	No adjustments	No adjustments
Step 4 System: Categorization	Low	Moderate	Low
	Overall Information System Impact: Moderate		

Step 2: Select Security Controls

Once data contents are mapped onto the information types in step 1, an overall impact rating (L-M-H) is determined for the dataset or information system as a whole. The impact rating drives step two of the RMF process, "select security controls". The impact rating determines the minimum number of controls required to safeguard the system and mitigate risk.

NIST SP 800-53 catalogues the 633 controls by control family. Each control is designed to address risk associated with one of the three security objectives (C-I-A). The combination of controls selected is what secures and protects the system at low, moderate or high levels. Table 5 summarizes the NIST publications that guide the selection of controls. Table 6 summarizes the total number of controls defined in each family and the minimum number of controls required for each security categorization.

Table 5: NIST Publications for Step 2 – Select Controls

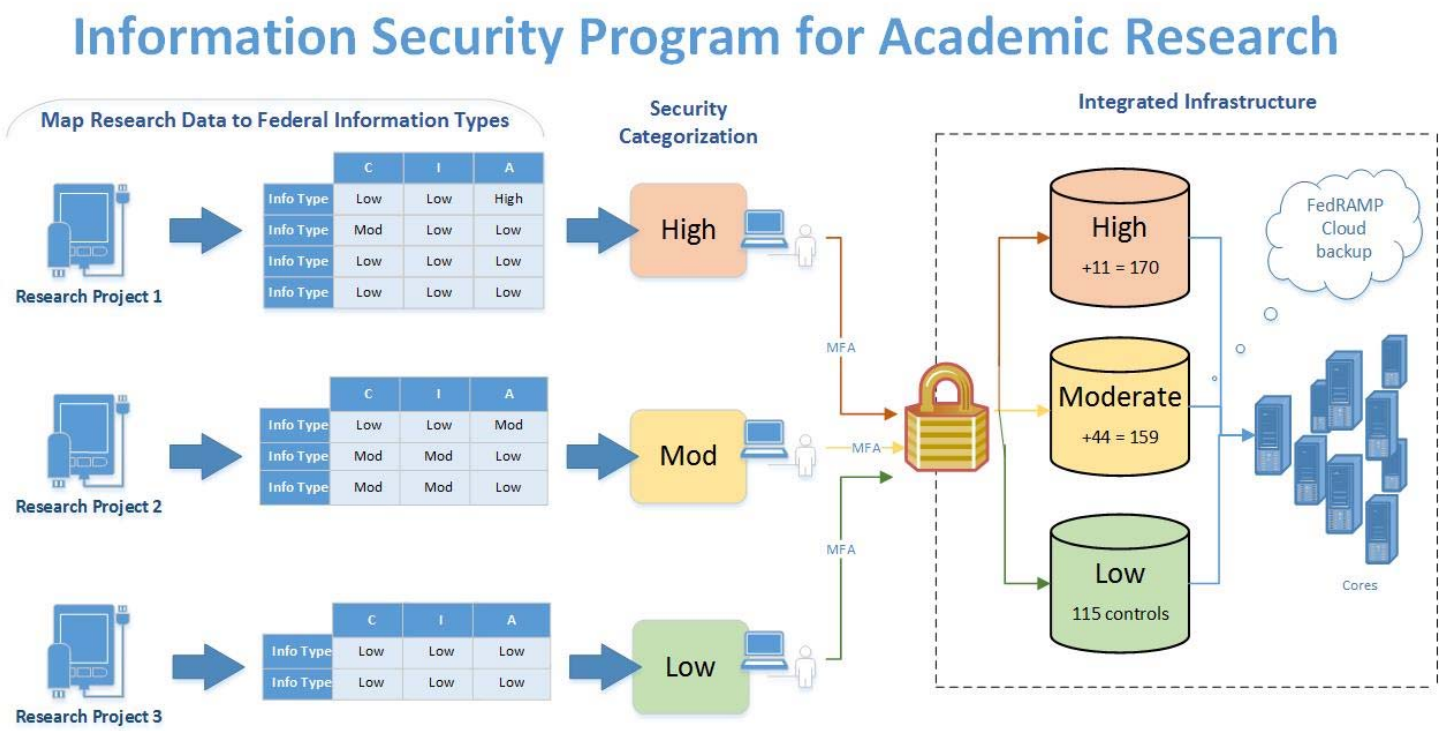
NIST Publication Number	NIST Publication Title	Key Points
FIPS200 (17 pages)	Minimum Security Requirements for Federal Information and Information Systems	-Defines the 18 security control families -Explains how the FIPS199 security categorization (L-M-H) links to SP 800-53 baseline controls
SP 800-53 (462 pages)	Security and Privacy Controls for Federal Information Systems and Organizations	-Section 3 outlines the process to: 1-select a security control baseline, 2-tailor the baseline, 3-document the selection process -Appendix F: Comprehensive catalogue of the 633 controls and control enhancements

Table 6: Number of NIST Security Controls by Family (Total and Minimum Number per Security Categorization)

Control Family	Class	Total Controls	Low	Moderate	High
1. Access Control (AC)	Technical	90	11	35	43
2. Audit and Accountability (AU)	Technical	47	10	18	28
3. Awareness and Training (AT)	Operational	8	4	5	5
4. Configuration Management (CM)	Operational	42	8	21	31
5. Contingency Planning (CP)	Operational	46	6	22	35
6. Identification and Authentication (IA)	Technical	33	15	22	24
7. Incident Response (IR)	Operational	21	7	12	16
8. Maintenance (MA)	Operational	23	4	9	13
9. Media Protection (MP)	Operational	19	4	9	12
10. Personnel Security (PS)	Operational	12	8	8	9
11. Physical and Environmental Protection (PE)	Operational	49	10	18	26
12. Planning (PL)	Management	9	3	6	6
13. Program Management (PM)	Management	16	0	0	0
14. Risk Assessment (RA)	Management	14	4	7	8
15. Security Assessment and Authorization (CA)	Management	14	7	10	12
16. System and Communications Protection (SC)	Technical	95	10	24	30
17. System and Information Integrity (SI)	Operational	54	6	21	27
18. System and Services Acquisition (SA)	Management	41	7	14	18
Total Number of Controls		**633**	**124**	**261**	**343**

Documenting the research landscape at academic institutions is important for system architecture and design. If an institution's research portfolio is funded primarily by federal sponsors, further analysis is needed to understand the breadth and depth of regulated data.

Integrated infrastructure for regulated data can be designed to accommodate varying degrees of security and privacy controls. Once the security categorization is complete, academic research projects are easily moved into pre-assessed computing environments, as depicted in Diagram 3:



Contributors from the University of Florida

Executive Sponsors

- UF Information Technology
  - Elias G. Eldayrie, MBA, Vice President & Chief Information Officer
  - Rob Adams, Chief Information Security Officer
  - Erik Deumens, PhD, Director of Research Computing
- UF Office of Research
  - David Norton, PhD, Vice President for Research
  - Stephanie Gray, MBA, Assistant Vice President & Director of Sponsored Programs
  - Irene M. Cooke, DVM, PhD, Director of Research Compliance
- UF Department of Health Outcomes and Policy
  - Elizabeth A. Shenkman, PhD, Professor, Department Chair, and Director, Institute for Child Health Policy
  - Deepa Ranka, PhD, Lecturer & Faculty
  - Ashley Sanders, MS, Assistant Director, Research Programs
- Donna Carden, MD, Director of Faculty Development and Professor, UF Department of Emergency Medicine
- Susan Blair, MSJ, MBA, UF Chief Privacy Officer
- Amy M. Haas, JD, Executive Associate Vice President, UF Deputy General Counsel
- Ron Ross, PhD, Computer Scientist, NIST Fellow, FISMA Project Leader

UF Implementation Team

- Project Managers: Tricia Cook (Lead), Dianne Swancinger, Troy Haynes, Stephen Cates
- Operations: Scott Crowell, David Stricklin, Brian Parks, Rodger Hendricks
- Information Security: Cheryl Granto, Avi Baumstein, Chris Cuevas, Derrius Marlin
- Business Relationship Manager: Alicia Turner
- Database Administrator: James Martinez
- Citrix: Michael Kutyna, Nicholas Cecere, Shannon Forest, Tom Wright
- Identity Access Management: Diane Weigle, Kerry Bader
- Network Services: James Oulman, Joe Gasper, Andrew Carey, Paul Smith, Logan Clapp, Eli Ben-Shoshan, Allen Rout

Appendix A: Federal Information Types and NIST Impact Ratings

Mission Based Information Types (94 total)

800-60 Order	Federal Line of Business	Federal Information Type	Confidentiality	Integrity	Availability
1	(not defined)	Defense & National Security	Nat'l Security	Nat'l Security	Nat'l Security
2	Homeland Security	Border Control and Transportation Security	Moderate	Moderate	Moderate
3	Homeland Security	Key Asset and Critical Infrastructure Protection	High	High	High
4	Homeland Security	Catastrophic Defense	High	High	High
5	Homeland Security	Executive Functions of the EOP	High	Moderate	High
6	Homeland Security	Intelligence Operations	High	High	High
7	Disaster Management	Disaster Monitoring and Prediction	Low	High	High
8	Disaster Management	Disaster Preparedness and Planning	Low	Low	Low
9	Disaster Management	Disaster Repair and Restoration	Low	Low	Low
10	Disaster Management	Emergency Response	Low	High	High
11	International Affairs and Commerce	Foreign Affairs	High	High	Moderate
12	International Affairs and Commerce	International Development and Humanitarian Aid	Moderate	Low	Low
13	International Affairs and Commerce	Global Trade	High	High	High
14	Natural Resources	Water Resource Management	Low	Low	Low
15	Natural Resources	Conservation, Marine, and Land Management	Low	Low	Low
16	Natural Resources	Recreational Resource Management and Tourism	Low	Low	Low
17	Natural Resources	Agricultural Innovation and Services	Low	Low	Low
18	Energy	Energy Supply	Low	Moderate	Moderate
19	Energy	Energy Conservation and Preparedness	Low	Low	Low
20	Energy	Energy Resource Management	Moderate	Low	Low
21	Energy	Energy Production	Low	Low	Low
22	Environmental Management	Environmental Monitoring/ Forecasting	Low	Moderate	Low
23	Environmental Management	Environmental Remediation	Moderate	Low	Low
24	Environmental Management	Pollution Prevention And Control	Low	Low	Low
25	Economic Development	Business and Industry Development	Low	Low	Low
26	Economic Development	Intellectual Property Protection	Low	Low	Low
27	Economic Development	Financial Sector Oversight	Moderate	Low	Low

28	Economic Development	Industry Sector Income Stabilization	Moderate	Low	Low
29	Community and Social Services	Homeownership Promotion	Low	Low	Low
30	Community and Social Services	Community and Regional Development	Low	Low	Low
31	Community and Social Services	Social Services	Low	Low	Low
32	Community and Social Services	Postal Services	Low	Moderate	Moderate
33	Transportation	Ground Transportation	Low	Low	Low
34	Transportation	Water Transportation	Low	Low	Low
35	Transportation	Air Transportation	Low	Low	Low
36	Transportation	Space Operations	Low	High	High
37	Education	Elementary, Secondary, and Vocational Education	Low	Low	Low
38	Education	Higher Education	Low	Low	Low
39	Education	Cultural & Historic Preservation	Low	Low	Low
40	Education	Cultural & Historic Exhibition	Low	Low	Low
41	Workforce Management	Training and Employment	Low	Low	Low
42	Workforce Management	Labor Rights Management	Low	Low	Low
43	Workforce Management	Worker Safety	Low	Low	Low
44	Health	Access to Care	Low	Moderate	Low
45	Health	Population Health Management and Consumer Safety	Low	Moderate	Low
46	Health	Health Care Administration	Low	Moderate	Low
47	Health	Health Care Delivery Services	Low	High	Low
48	Health	Health Care Research and Practitioner Education	Low	Moderate	Low
49	Income Security	General Retirement and Disability	Moderate	Moderate	Moderate
50	Income Security	Unemployment Compensation	Low	Low	Low
51	Income Security	Housing Assistance	Low	Low	Low
52	Income Security	Food and Nutrition Assistance	Low	Low	Low
53	Income Security	Survivor Compensation	Low	Low	Low
54	Law Enforcement	Criminal Apprehension	Low	Low	Moderate
55	Law Enforcement	Criminal Investigation and Surveillance	Moderate	Moderate	Moderate
56	Law Enforcement	Citizen Protection	Moderate	Moderate	Moderate
57	Law Enforcement	Leadership Protection	Moderate	Low	Low
58	Law Enforcement	Property Protection	Low	Low	Low
59	Law Enforcement	Substance Control	Moderate	Moderate	Moderate
60	Law Enforcement	Crime Prevention	Low	Low	Low
61	Law Enforcement	Trade Law Enforcement	Moderate	Moderate	Moderate

62	Litigation and Judicial Activities	Judicial Hearings	Moderate	Low	Low
63	Litigation and Judicial Activities	Legal Defense	Moderate	High	Low
64	Litigation and Judicial Activities	Legal Investigation	Moderate	Moderate	Moderate
65	Litigation and Judicial Activities	Legal Prosecution and Litigation	Low	Moderate	Low
66	Litigation and Judicial Activities	Resolution Facilitation	Moderate	Low	Low
67	Federal Correctional Activities	Criminal Incarceration	Low	Moderate	Low
68	Federal Correctional Activities	Criminal Rehabilitation	Low	Low	Low
69	General Science and Innovation	Scientific and Technological Research and Innovation	Low	Moderate	Low
70	General Science and Innovation	Space Exploration and Innovation	Low	Moderate	Low
71	Knowledge Creation and Management	Research and Development	Low	Moderate	Low
72	Knowledge Creation and Management	General Purpose Data and Statistics	Low	Low	Low
73	Knowledge Creation and Management	Advising and Consulting	Low	Low	Low
74	Knowledge Creation and Management	Knowledge Dissemination	Low	Low	Low
75	Regulatory Compliance and Enforcement	Inspections and Auditing	Moderate	Moderate	Low
76	Regulatory Compliance and Enforcement	Standards Setting/ Reporting Guideline Development	Low	Low	Low
77	Regulatory Compliance and Enforcement	Permits and Licensing	Low	Low	Low
78	Public Goods Creation and Management	Manufacturing	Low	Low	Low
79	Public Goods Creation and Management	Construction	Low	Low	Low
80	Public Goods Creation and Management	Public Resources, Facility, and Infrastructure Management	Low	Low	Low
81	Public Goods Creation and Management	Information Infrastructure Management	Low	Low	Low
82	Federal Financial Assistance	Federal Grants (Non-State)	Low	Low	Low
83	Federal Financial Assistance	Direct Transfers to Individuals	Low	Low	Low
84	Federal Financial Assistance	Subsidies	Low	Low	Low
85	Federal Financial Assistance	Tax Credits	Moderate	Low	Low
86	Credits and Insurance	Direct Loans	Low	Low	Low
87	Credits and Insurance	Loan Guarantees	Low	Low	Low
88	Credits and Insurance	General Insurance	Low	Low	Low

89	Transfers to State/Local Governments	Formula Grants	Low	Low	Low
90	Transfers to State/Local Governments	Project/Competitive Grants	Low	Low	Low
91	Transfers to State/Local Governments	Earmarked Grants	Low	Low	Low
92	Transfers to State/Local Governments	State Loans	Low	Low	Low
93	Direct Services for Citizens	Military Operations	N/A	N/A	N/A
94	Direct Services for Citizens	Civilian Operations	N/A	N/A	N/A

Management and Support Information Types (77 total)

800-60 Order	Federal Line of Business	Federal Information Type	Confidentiality	Integrity	Availability
95	Controls and Oversight	Corrective Action (Policy/Regulation)	Low	Low	Low
96	Controls and Oversight	Program Evaluation	Low	Low	Low
97	Controls and Oversight	Program Monitoring	Low	Low	Low
98	Regulatory Development	Policy and Guidance Development	Low	Low	Low
99	Regulatory Development	Public Comment Tracking	Low	Low	Low
100	Regulatory Development	Regulatory Creation	Low	Low	Low
101	Regulatory Development	Rule Publication	Low	Low	Low
102	Planning and Budgeting	Budget Formulation	Low	Low	Low
103	Planning and Budgeting	Capital Planning	Low	Low	Low
104	Planning and Budgeting	Enterprise Architecture	Low	Low	Low
105	Planning and Budgeting	Strategic Planning	Low	Low	Low
106	Planning and Budgeting	Budget Execution	Low	Low	Low
107	Planning and Budgeting	Workforce Planning	Low	Low	Low
108	Planning and Budgeting	Management Improvement	Low	Low	Low
109	Planning and Budgeting	Budgeting & Performance Integration	Low	Low	Low
110	Planning and Budgeting	Tax and Fiscal Policy	Low	Low	Low
111	Internal Risk and Mitigation	Contingency Planning	Moderate	Moderate	Moderate
112	Internal Risk and Mitigation	Continuity of Operations	Moderate	Moderate	Moderate
113	Internal Risk and Mitigation	Service Recovery	Low	Low	Low
114	Revenue Collection	Debt Collection	Moderate	Low	Low
115	Revenue Collection	User Fee Collection	Low	Low	Moderate
116	Revenue Collection	Federal Asset Sales	Low	Moderate	Low
117	Public Affairs	Customer Services	Low	Low	Low
118	Public Affairs	Official Information Dissemination	Low	Low	Low
119	Public Affairs	Product Outreach	Low	Low	Low

120	Public Affairs	Public Relations	Low	Low	Low
121	Legislative Relations	Legislation Tracking	Low	Low	Low
122	Legislative Relations	Legislation Testimony	Low	Low	Low
123	Legislative Relations	Proposal Development	Moderate	Low	Low
124	Legislative Relations	Congressional Liaison Operations	Moderate	Low	Low
125	General Government	Central Fiscal Operations	Moderate	Low	Low
126	General Government	Legislative Functions	Low	Low	Low
127	General Government	Executive Functions	Low	Low	Low
128	General Government	Central Property Management	Low	Low	Low
129	General Government	Central Personnel Management	Low	Low	Low
130	General Government	Taxation Management	Moderate	Low	Low
131	General Government	Central Records and Statistics Management	Moderate	Low	Low
132	General Government	Income Information	Moderate	Moderate	Moderate
133	General Government	Personal Identity and Authentication	Moderate	Moderate	Moderate
134	General Government	Entitlement Event Information	Moderate	Moderate	Moderate
135	General Government	Representative Payee Information	Moderate	Moderate	Moderate
136	General Government	General Information9	Low	Low	Low
137	Administrative Management	Facilities, Fleet, and Equipment Management	Low	Low	Low
138	Administrative Management	Help Desk Services	Low	Low	Low
139	Administrative Management	Security Management	Moderate	Moderate	Low
140	Administrative Management	Travel	Low	Low	Low
141	Administrative Management	Workplace Policy Development and Management	Low	Low	Low
142	Financial Management	Asset and Liability Management	Low	Low	Low
143	Financial Management	Reporting and Information	Low	Moderate	Low
144	Financial Management	Funds Control	Moderate	Moderate	Low
145	Financial Management	Accounting	Low	Moderate	Low
146	Financial Management	Payments	Low	Moderate	Low
147	Financial Management	Collections and Receivables	Low	Moderate	Low
148	Financial Management	Cost Accounting/ Performance Measurement	Low	Moderate	Low
149	Human Resource Management	HR Strategy	Low	Low	Low
150	Human Resource Management	Staff Acquisition	Low	Low	Low
151	Human Resource Management	Organization and Position Management	Low	Low	Low

152	Human Resource Management	Compensation Management	Low	Low	Low
153	Human Resource Management	Benefits Management	Low	Low	Low
154	Human Resource Management	Employee Performance Management	Low	Low	Low
155	Human Resource Management	Employee Relations	Low	Low	Low
156	Human Resource Management	Labor Relations	Low	Low	Low
157	Human Resource Management	Separation Management	Low	Low	Low
158	Human Resource Management	Human Resources Development	Low	Low	Low
159	Supply Chain Management	Goods Acquisition	Low	Low	Low
160	Supply Chain Management	Inventory Control	Low	Low	Low
161	Supply Chain Management	Logistics Management	Low	Low	Low
162	Supply Chain Management	Services Acquisition	Low	Low	Low
163	Information and Technology Management	System Development	Low	Moderate	Low
164	Information and Technology Management	Lifecycle/Change Management	Low	Moderate	Low
165	Information and Technology Management	System Maintenance	Low	Moderate	Low
166	Information and Technology Management	IT Infrastructure Maintenance	Low	Low	Low
167	Information and Technology Management	Information System Security	Low	Moderate	Low
168	Information and Technology Management	Record Retention	Low	Low	Low
169	Information and Technology Management	Information Management	Low	Moderate	Low
170	Information and Technology Management	System and Network Monitoring	Moderate	Moderate	Low
171	Information and Technology Management	Information Sharing	N/A	N/A	N/A