FEDERAL DEMONSTRATION PARTNERSHIP

Redefining the Government & University Research Partnership

FISMA
What is it and how can you be prepared

Dr. Ron Ross, NIST

Alicia Turner, University of Florida

FEDERAL DEMONSTRATION PARTNERSHIP

Redefining the Government & University Research Partnership

FISMA at UF

Alicia Turner, Business Relationship Manager

Enterprise Systems, UF Information Technology (UFIT)

FISMA at UF

- UF FISMA Overview
  - Architecture
  - Implementation
  - Next steps
- Lessons learned
- Unanswered questions

UF FISMA Executive Sponsors

- Rob Adams, Chief Information Security Officer
- Susan Blair, Chief Privacy Officer
- Erik Deumens, Research Computing Director
- Elias Eldayrie, Chief Information Officer
- Stephanie Gray, Director of Sponsored Programs
- David Norton, Vice President for Research

Architecture Overview

UF Research Shield (ResShield) “went live” in July 2015 and provides a research computing environment compliant with NIST moderate IT/security controls

- A “data center within a data center”
- Multi-tenant design
- VPN to VDI via MFA
- 300 total controls (170 leveraged + 130 new)
- Security Technical Implementation Guides (STIGs)

“Data Center within a Data Center”

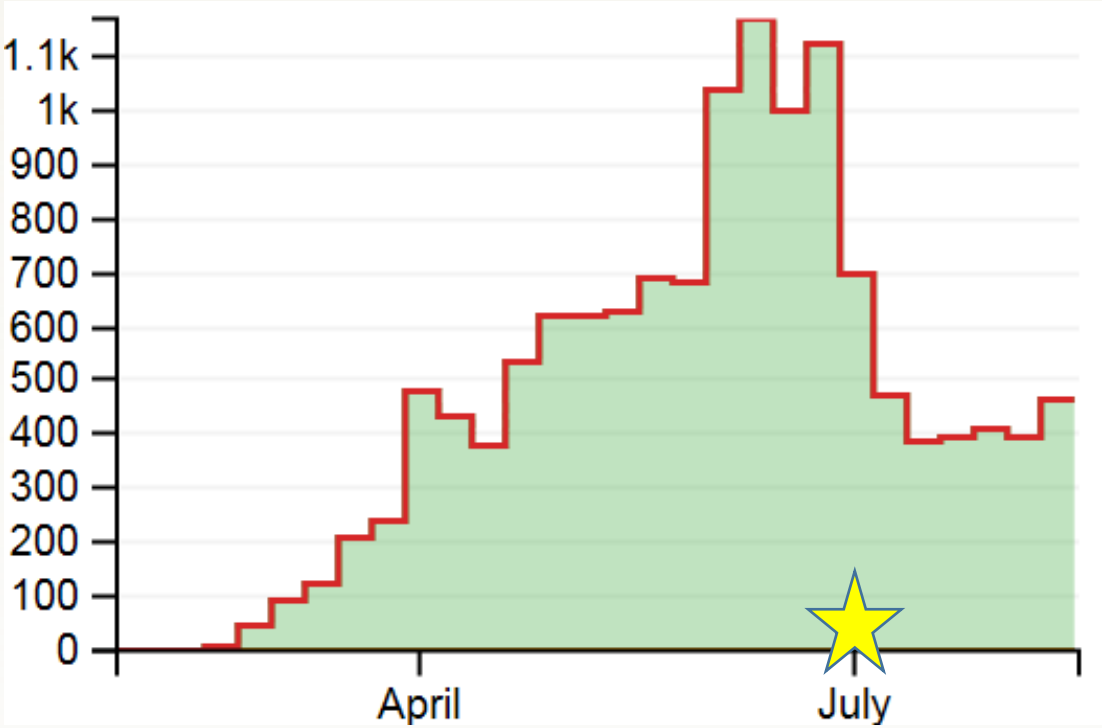
Implementation Overview

UFIT sponsored and invested in ResShield to ensure compliance with a $40M Medicaid data analytics contract

- $2M investment
- 80 UFIT employees
- Over 13,000 man hours (6 man years)
- Third Party Assessment Organization (3PAO)

Deployment Timeline

UF FISMA - Project Implementation Hours by Month



Implementation Budget

Budget Category	Year One Amount	Annual Recurring	5 Year TCO
Hardware	672,379	85,866	1,015,843
Software	233,901	123,964	729,758
Facility	58,596	0	58,596
Other	870	0	870
Consulting	499,001	25,000	599,001
New FTE	49,064	265,400	1,110,664
Total	**1,513,811**	**500,230**	**3,514,732**

Note: budget figures as of July 28, 2015

Project Stakeholders

Office of Research (OR)	• Review and endorse all FISMA proposal submissions • Negotiate and accept terms and conditions of contract (and modifications) • Serve as the primary point of contact for interactions and communications with the government's Contracting Officer
General Counsel (GC)	• Serve in advisory capacity for legal issues.
Privacy Office (PO)	• Provide services to conduct a Privacy Impact Assessment (PIA) • Review and endorse all FISMA proposal submissions • Provide Subject Matter Expertise on privacy regulations and requirements
Principal Investigator (PI)	• Develop science and work with OR, CPO, UFIT and GC to complete proposal paperwork • Interact/contact with the government's Contracting Officer's Representative with respect to technical issues related to the contract
Security Office & UFIT	• Provide Information Security Risk Assessment, Business Impact Assessment, and Information Classification deliverables • Provide signatory authority for IT specific FISMA deliverables • Provide post-award technical project management and implementation services as well as own and operate services

Why invest?

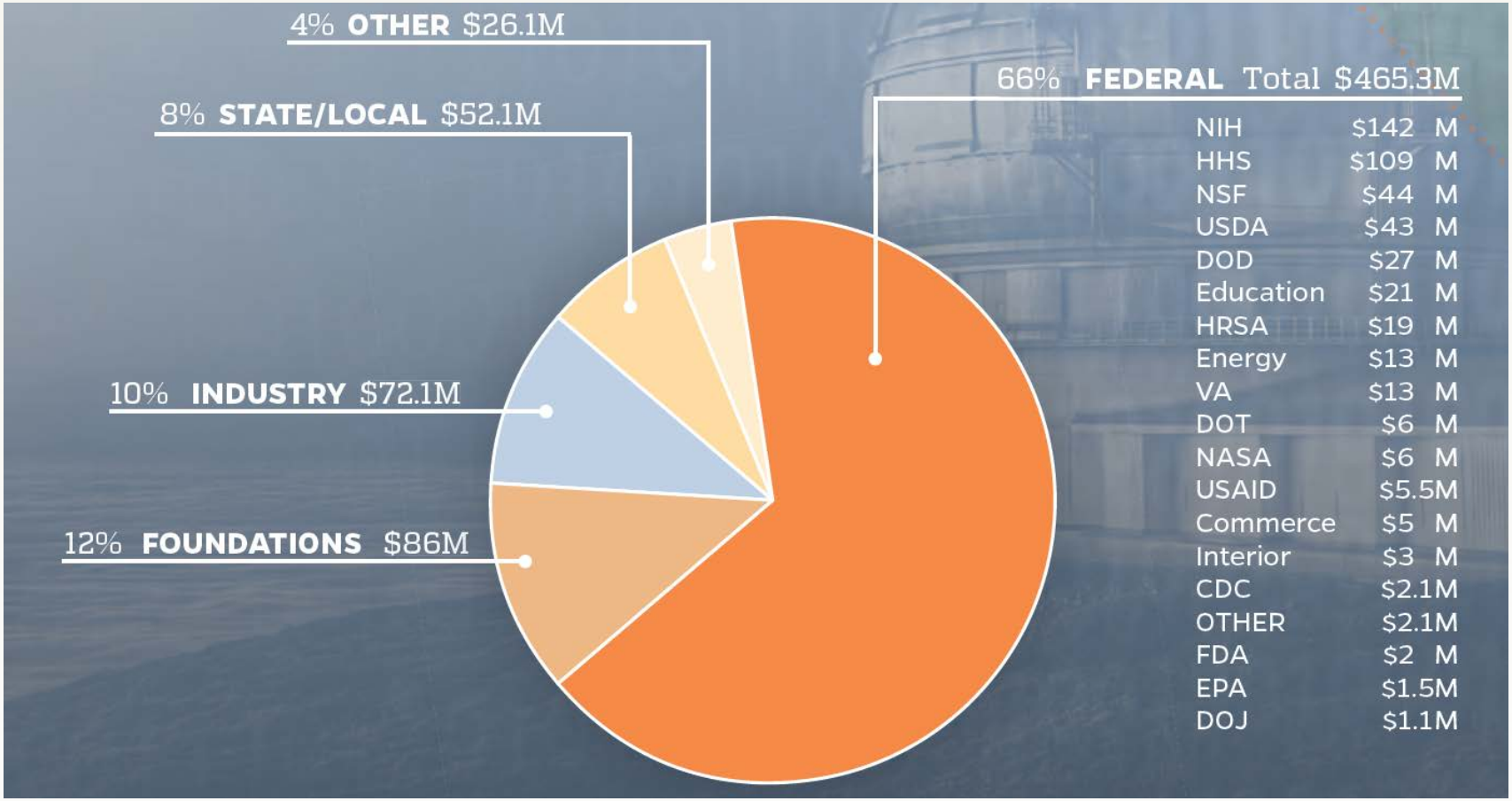
- **Driving Force:** $40M Medicaid data analytics contract
- Notable increase in FISMA/NIST contract terms and conditions
- UF spotlight on information security & increased effort for privacy/risk assessments
- But perhaps the most important reason…

UF Research Portfolio

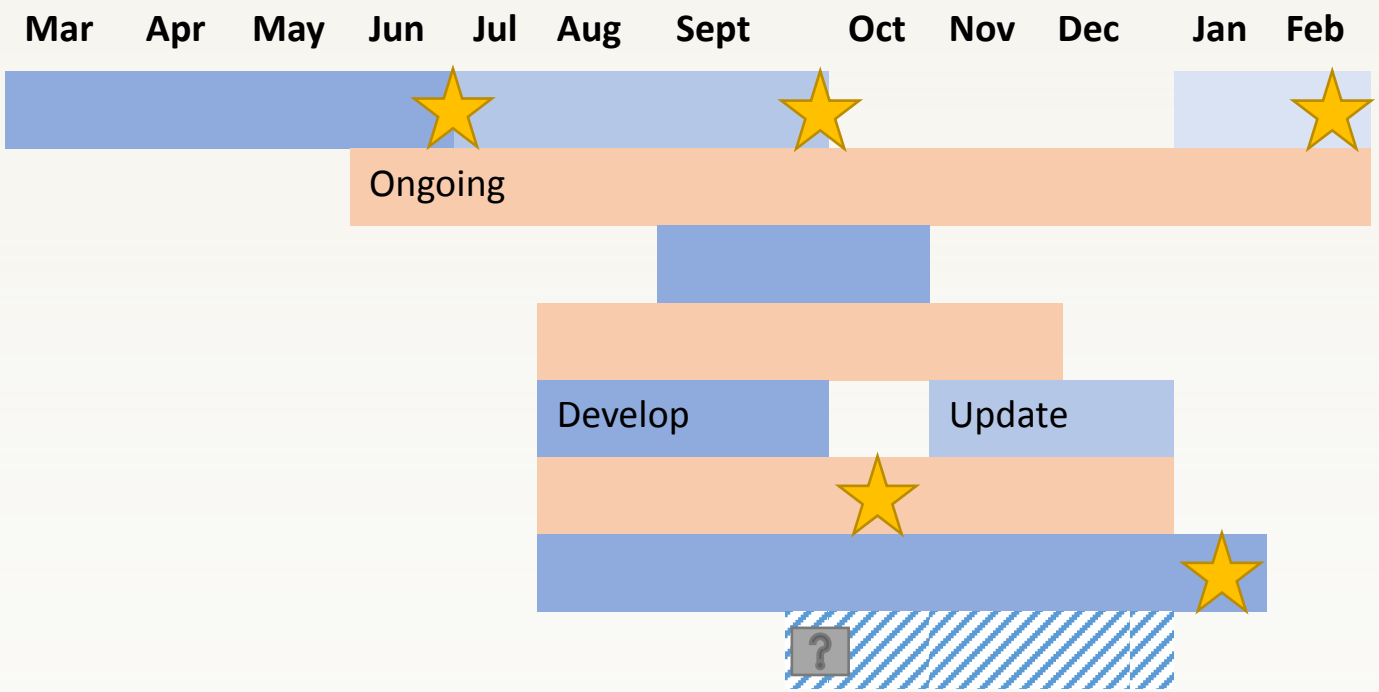
UF Office of Research Annual Report

FY2014 Total Research Revenue: $702M

(FY2015 Total Research Revenue: $706M)



Next steps for FISMA at UF



*Two major activities for the ResShield implementation and onboarding:

1. Technical build (most is “one time”)
2. Documentation (repeats with each tenant)

UF Vision:
Integrated Infrastructure for Regulated Data

Examples	Supporting Regulation	Security Standards	*Min # of Controls
HIPAA	HIPAA	DHHS	22
Controlled Technical Information (CTI)	DFAR 7012 ITAR/EAR	*NIST SP 800-53	51
Controlled Unclassified Information (CUI)	*NARA pending	NIST SP 800-171	109
NIST Low	FISMA	NIST FIPS & SP	115
NIST Moderate	FISMA	NIST FIPS & SP	159
NIST High	FISMA	NIST FIPS & SP	170
UF "deemed" restricted data (but not required in contract terms)	N/A	?	?

**Minimum # of controls do not include control enhancements*
**Proposed revision to DFAR 7012 would require NIST SP 800-171*
**Proposed NARA regulation would require NIST SP 800-171 for all CUI*

Lessons Learned (1 of 4)

Note that our first tenant was an exception:

FISMA Tenant	FISMA Required By	Start Date	Size	Users	External Partners	General Apps	Specialty Apps	Databases	DMZ	Outbound PHI/PII?
Tenant 1	1 Contract	Jul 2015	39TB	60	9+MCO	37	11	10	Yes	Yes
Tenant 2	2 Contracts	Oct 2015	20TB	6	2	<10	1	3-5	No	No
Tenant 3	CMS DUA	Dec 2015	5 GB	6	2	<10	0	2	No	No

Lessons Learned (2 of 4)

Security standards are very subjective and there's more than one way to skin the 'implementation cat'

- Learn enough to form your own opinion
- Push back on sponsors that use generic terms
- Compliance does not equal security!

Lessons Learned (3 of 4)

In a nutshell, plan thoroughly before you build (4-6 months minimum)

- Form strategic planning group w/ major stakeholders early in the process
- Security controls 101
  - Take the time to learn them (all project stakeholders!)
  - Understand what you already have that can be leveraged
- Assess your research landscape
  - What volume requires information security scrutiny/interpretation?
  - What agencies can “talk NIST”?
- Design infrastructure/architecture that scales easily and builds in cost efficiencies

Lessons learned (4 of 4)

Support the business, don't "interrupt" the business

- Train staff
  - Identify, interpret, negotiate "down or out"
  - Direct regulated data to the appropriate environment
- Best practices for efficient/expedient privacy and risk assessments
- Incorporate economic indicators to gauge financial loss/risk

Unanswered Questions

- Does regulation apply to primary datasets, secondary datasets, or both?
- How should we handle sponsors or data providers that don't understand FIPS199 and/or push back on providing the security categorization?
- There is an obvious disconnect between sponsors and data providers, how do we get data security requirements to appear in RFA/FOA?