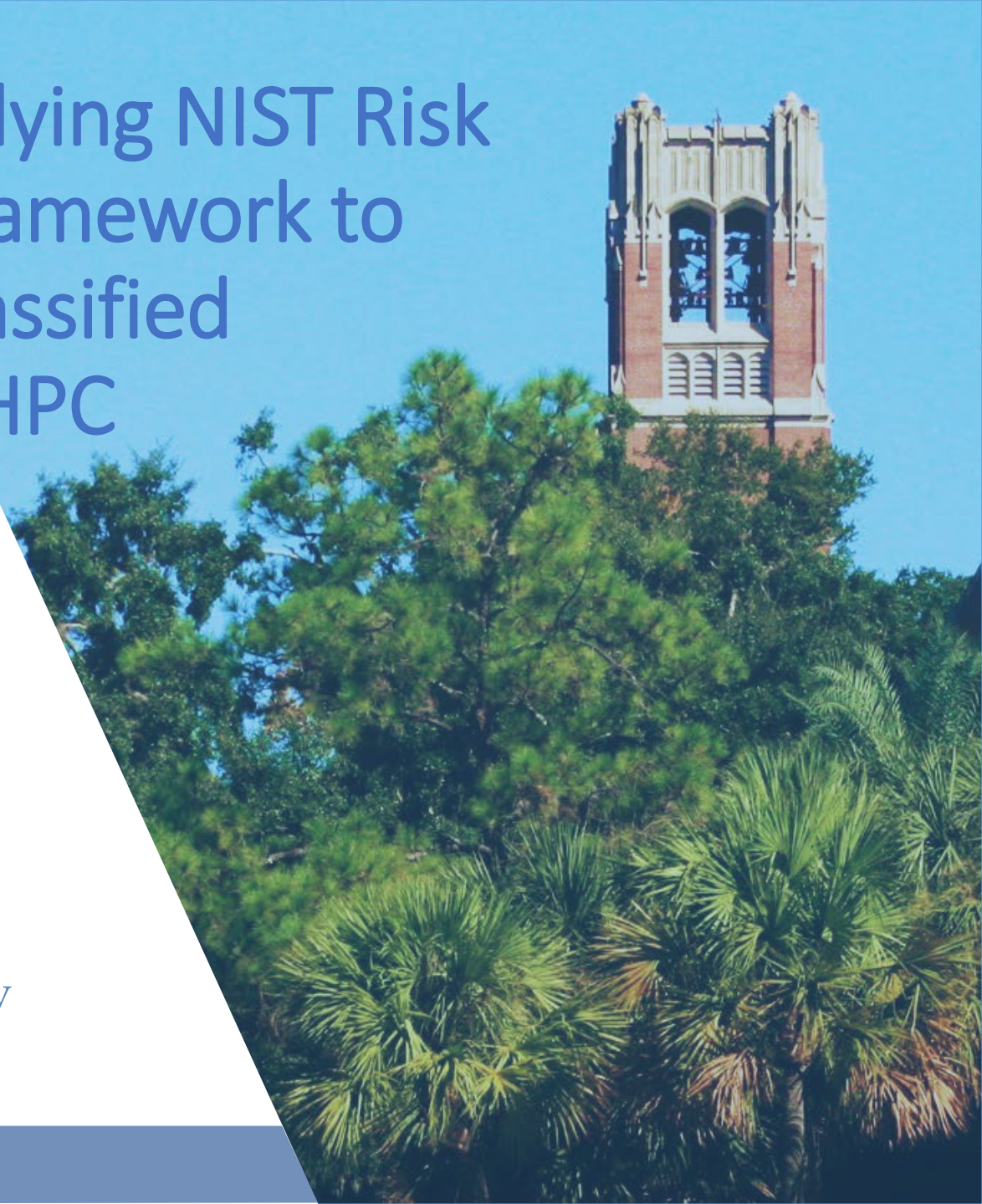
Case Study: Applying NIST Risk Management Framework to Controlled Unclassified Information on HPC



NIST High-Performance computing workshop

Mar 27-28, 2018

Gaithersburg, MD

Erik Deumens

Research Computing director

UF | Information Technology

Part 1: Regulatory Requirements

Controlled Unclassified Information (CUI)

CUI is information that law, regulation, or government wide policy requires to have safeguarding or disseminating controls[1]

Replaces many previous federal designations, such as SBU, LES, FOUO & SSI

CUI has the same value, whether such information is resident in a federal system that is part of a federal agency or a nonfederal system that is part of a nonfederal organization[2]

Statutory and regulatory requirements for the protection of CUI are consistent, whether such information resides in federal information systems or nonfederal information system

[1]Executive Order 13566

[2]NIST Special Publication 800-171 Revision 1

What is the Federal Strategy for Protecting CUI?

- Federal CUI rule (32 CFR Part 2002) establishes the required controls and markings for CUI government wide
- NIST Special Publication 800-171 defines security requirements for protecting CUI in nonfederal information systems and organizations
- Federal Acquisition Regulation (FAR) clause to apply the requirements of the federal CUI rule and SP 800-171 to nonfederal organizations (planned for 2017)

NIST Special Publication 800-171

"Protecting CUI in Non-Federal Information Systems and Organizations" - June 18, 2015

- Applies to all components of nonfederal systems and organizations that process, store, or transmit CUI
- Intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations
- Focuses on protecting the confidentiality of CUI in nonfederal systems and organizations
- Assumes that the confidentiality impact value for CUI is no lower than moderate

FAR and DFARS Safeguarding Clauses
Showing up in Contract Terms

- **Federal Acquisition Regulation (FAR) 52.204-21 – Basic Safeguarding of Contractor Information Systems**

Applies to all fed contracts, not as restrictive as CUI

- Effective June 15, 2016
- Department of Defense (DoD), General Services Administration (GSA), and National Aeronautics and Space Administration (NASA)
- Requires safeguarding requirements with comparable security requirements from NIST SP 800-171

- **Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 – Network Penetration Reporting and Contracting for Cloud Services**
  - Effective October 21, 2016
  - Department of Defense (DoD)
  - Requires the implementation of the security requirements in NIST SP 800-171
  - Deadline is December 31, 2017

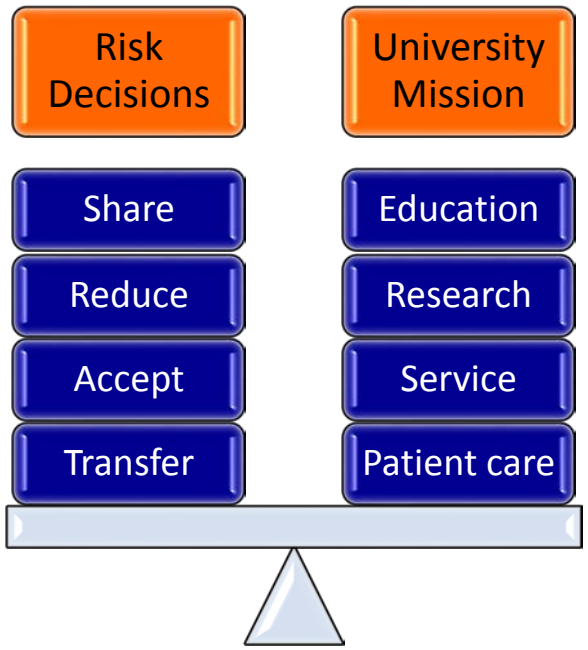
Part 2: Institutional Effort

Institutional Collaboration

Build Trust
&
Develop Long-Term Partnerships

- Faculty
- VPR & Office of Research
- VP/CIO & Information Technology
- Support from President, Provost, COO for Risk Management
- Distributed Campus IT Units
- CISO & Information Security Office
- Privacy Office
- Office of Internal Audit
- Research Computing

Risk Management, Security, and Compliance



- Information security
  - Reduce chance of unauthorized data access and change.
  - Ensure unauthorized data access is recorded.
- Compliance
  - Provide a continuous record of security measures to show due diligence.
  - Ensure that an auditable record exists of any incidents.

Enable UF Researchers to Create New Technologies, Discover Industry Breakthroughs, and Spawn New Economic Opportunities

How do we abstract and secure the user interface layer to allow our research faculty to uncover ideas that change the world without having to understand regulatory compliance, information technology, information security and risk management?

Part 3: NIST framework

Manage risk

- Use Special Publication series 800 as library
- Organization focus
- SP 800-39 Organization, mission, and information system view
  - Need for correct scope for making decisions
- SP 800-37 Guide to applying RMF to federal IS
- SP 800-65 Capital planning and investment control
- SP 800-30 Guide to conducting risk assessments

Plan, architect, build a system

- System focus
- Classify for “moderate baseline”: FIPS 200
  - Maximize common controls
- Build, design, engineer: SP 800-160 v1 and v2
- Security controls: SP 800-53 and 171
- System security plan: SP 800-18
- Assessment: SP 800-26 self assessment guide
- Assessment: SP 800-53A and 171A

Manage projects

- Project focus
- Classify data: FIPS 199
- SP 800-60 v1 and v2
  - FISMA process
- NARA (National Archive and Registry Administration)
  - CUI process
- Provision projects in the system
- Inherit all common controls

Part 3: Implementation

Implementation principles

Meet Researcher Needs

- Affordable
- Reliable
- Easy to Provision
- Scale to many small projects
- Support large complex projects
- Simple to Use
- Or, as simple as possible

Simple Process

- Research requires nimbleness
- Include in project planning
- Or, proposal
- Or, when award is made
- Or, when data use agreement is processed
- Offer simple budget model

Enclave implementation option

- Create a pre-vetted environment
- Build, operate, and maintain as a system
  - Efficiency in hardware
  - Provision projects as they come up
- Test, monitor, audit, validate, and authorize as a system
  - Efficiency in staff effort
- Economy of scale and elasticity of capacity
  - Efficiency in cost

Nimble for research needs

- Cloud-like architecture
  - Not **self** provisioning
  - But **guided** provisioning
- Customization
  - Not full custom built
  - Still flexible to meet specific needs
- Strategy:
  - build once
  - deploy often
  - minimize customization

Optimize researcher time

- Bulk of compliance work is done by staff
  - From many departments, not just IT
- Researchers are not security & compliance officers
  - They do their part of the compliance

Business model fits research budgets

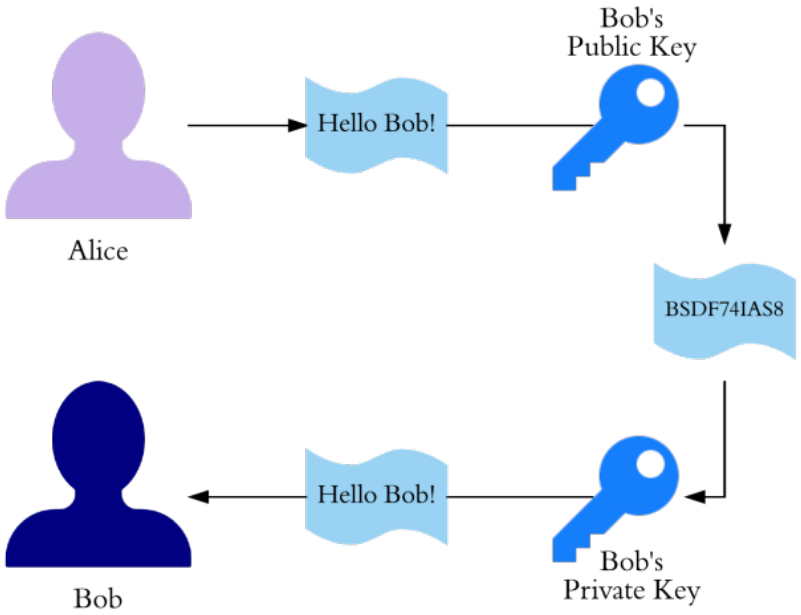
- Subsidized operation
- University pays for
  - Staff, data center, network, special infrastructure
- Faculty and grants pay for
  - Compute nodes
  - Storage systems, primary and backup

Ambitious Security Goals

- Protect users, data, work from the Administrators
  - Assume admin malicious of hackers took over the system
- Security Independent of Infrastructure
  - Assume SSL/TLS, VPN, firewalls have failed
- Easy to Use Despite Security Measures
  - Use web interfaces, integrated tools with no tedium

Is this even possible?

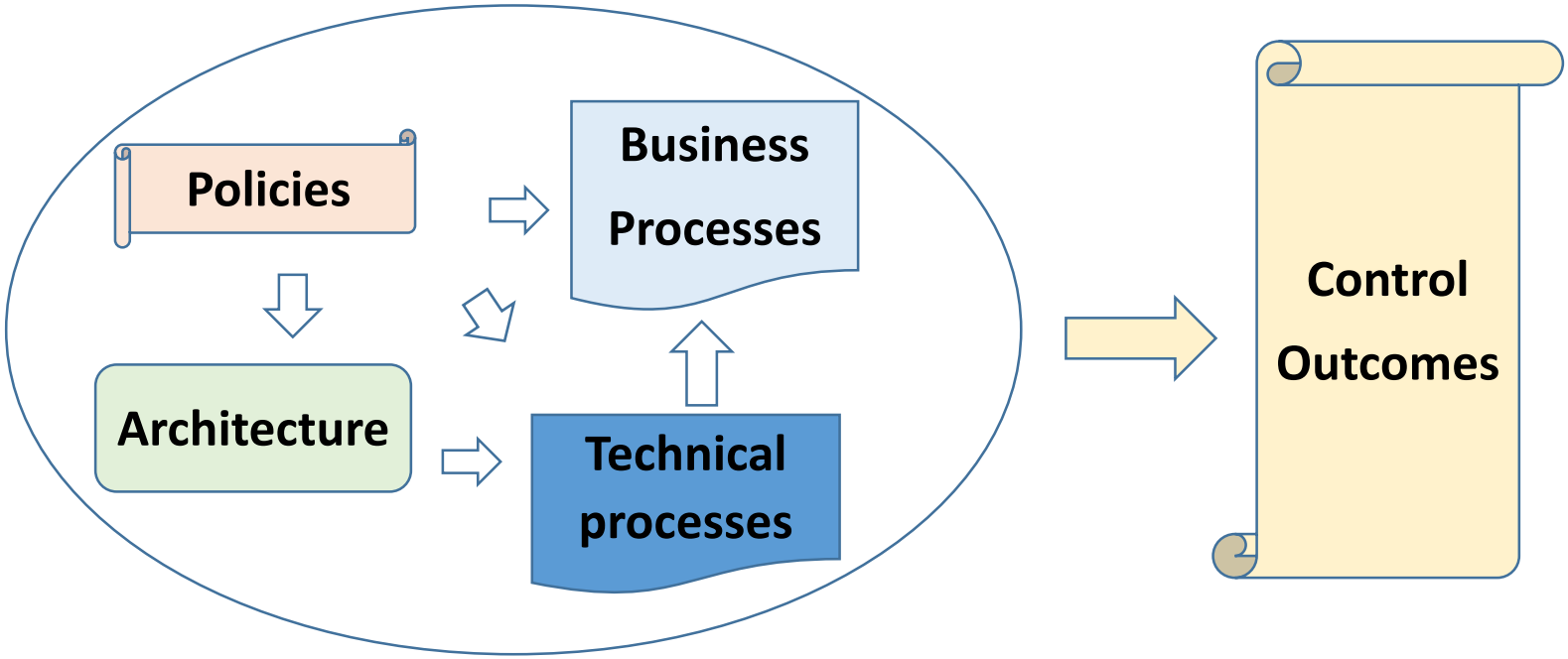
Public Key Cryptography Trusted technology



Formal build process

- Design and build
  - Involve institutional partners
- Review
  - Information Security Office
- Approve operation
  - Write system security plan (SSP)
  - Signed by CIO and CISO and system owner/operator
- Operate
  - Research Computing
  - Initial audit: 3rd party assessment organization (3PAO)
  - Annual audit: Office of Internal Audit

Compliance process



“Vertical” architecture

- Common in enterprise and cloud
- Tuned and dedicated infrastructure
  - Hypervisor manages VMs, storage in LUNs
- Defined, characterized, predictable workloads
- Provision systems for services
  - Use hypervisors, ACLs, VPNs to separate for confidentiality
  - Integrity and available is per VM
- This approach was used for ResShield in 2015
  - First generation system

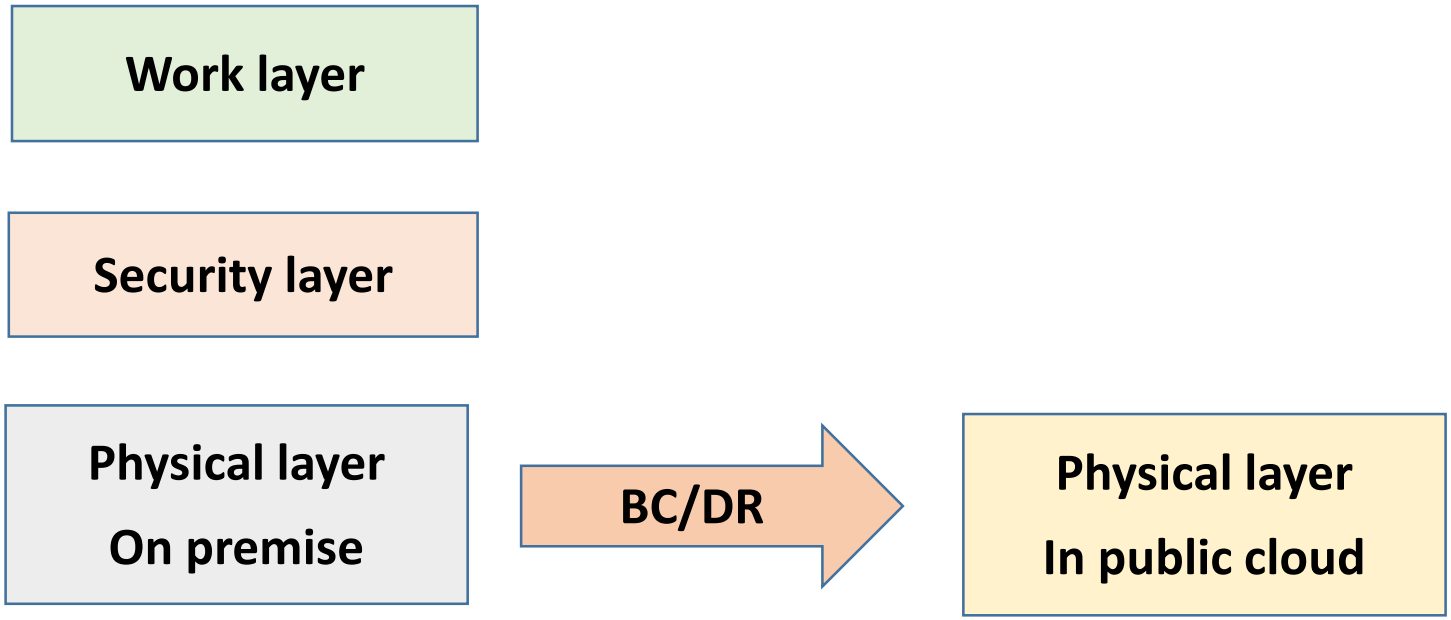
“Horizontal” architecture

- Typical in HPC
- Fast infrastructure: compute, storage, interconnect
- Flexible, demanding, unpredictable workloads
- Provision teams, groups, projects
  - Integrity and availability is common
  - Separation for confidentiality “late” in the stack
- This approach was used for ResVault in 2016-2017
  - Second generation system

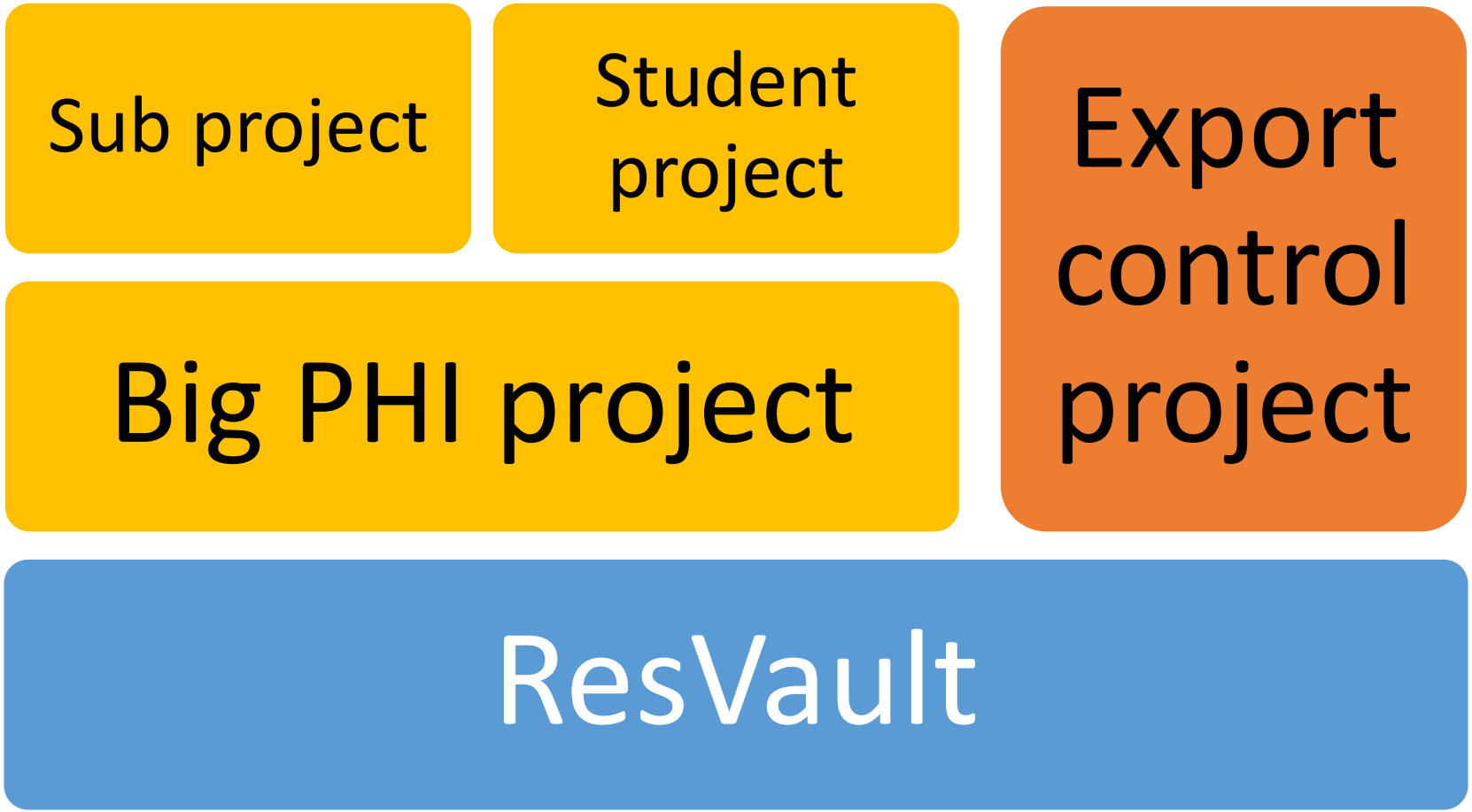
Technology in three layers

- Physical
  - Hardware servers and storage
  - On premise now, planning disaster recovery in public cloud
- Security
  - Built by Tera Insights with user groups in pilot projects
  - Provides “zero trust” end-to-end encryption
- Work
  - Research data storage and processing in secure VMs
  - Accessed with secure virtual desktop architecture

ResVault components



Project onboarding



What is next?

- We support small groups and collaborations
- We are building
  - Multi-user secure VMs
  - Secure clusters of secure VMs
- To address the need for
  - Servers, e.g. file and database, for large collaborations
  - Parallel processing with distributed memory
    - High-throughput computing
    - Big data analytics
    - MPI jobs (message passing interface)

Questions?

Secure Virtual Machines

Video of virtual machines