Cybersecurity in Research

Kairi Williams
Assistant Vice Chancellor for Research Administration & Compliance

April 13, 2022

The current environment…

- Higher education is already a target for cybersecurity threats.
- Many believe research data is the primary target.
- US Government concerns of foreign influence including cyber attacks.
- Increased regulations and use of DFAR clauses related to cybersecurity.
- $600M+ in annual federal awards

Federal cybersecurity requirements

- Cybersecurity Maturity Model Certification (CMMC)
  - CMMC is a U.S. Department of Defense (DoD) program that applies to Defense Industrial Base (DIB) contractors. It is a unifying standard and new certification model to ensure that DoD contractors properly protect sensitive information. CMMC introduces a new set of certifications, conducted by third-party assessors.
  - DOD recently announced CMMC 2.0 (3rd release in 5 years)
  - UC Berkeley DoD awards:
    - FY21- $48M
  - At least one project accepted in the last fiscal year that required certification.

NSPM-33

- National Security Presidential Memorandum -33 (NSPM-33)
  - Guidance released to federal agencies
  - The guidance specifically focuses on five key areas addressed by NSPM-33:
    - disclosure requirements and standardization
    - digital persistent identifiers
    - consequences for violation of disclosure requirements
    - information sharing
    - research security programs for institutions with $50M+ in federal funding
      - Foreign Travel Security
      - Research security training
      - Export control training, as appropriate
      - Cybersecurity

New NIH Data Management and Sharing

- The new policy applies to any researcher funded in whole or in part by NIH whose research generates scientific data, whereas the current policy only applies to grants requesting more than $500,000 of direct costs in a single year.

- The policy requires investigators to submit an official Data Management and Sharing Plan as part of their request for funding.

- Researchers will need to think ahead when planning research projects to take data sharing into consideration.

Challenges…

- Implementing cybersecurity requirements in an academic setting.
- No directly reimbursement from government for higher ed institutions.
- Impacts award setup time.
- Takes multiple departments and colleges to develop coordinated processes and advocacy for resources.
- Limited resources
  - Assessments/certifications
  - On going monitoring and compliance
  - Resources

Some ongoing and planned activities…

- Cybersecurity workgroup
- Rolling out IS-3 and IS-3 roles and responsibilities policies
- Once final, implementing Presidential Policy of Research Data
- Staying close to updates regarding NSPM-33 and research security program certification standards
- Assessing our current control environment to potential certification standards to identify significant gaps
- Enhance communications and awareness efforts to the research community

What we can do?

- Be an advocate
- Point PI's in the right direction
- Berkeley Research IT
  - Secure Research Data & Computing (research-it-consulting@lists.berkeley.edu)
  - Research Data Management Program (researchdata@berkeley.edu)

Questions?