Export Compliance Office

www.umresearch.umd.edu/Export
1204 Marie Mount Hall
Adam Grant: 301-405-4212; afgrant@umd.edu
What is Export Control?

International Traffic in Arms Regulations
The “ITAR”

Export Administration Regulations
The “EAR”

Office of Foreign Asset Controls
“OFAC”
ECO Services

- Foreign shipping and travel assistance
- Foreign Visit Requests
- Proposal/Contract Support
- Export licensing
- Technology Control Plans
- Training (Staff, Faculty, Departmental Liaisons)
- Proprietary information agreements
Federal Information Security Modernization Act of 2014 “FISMA”

- Mandate to protect federal information systems
- Updated from FISMA 2002
- OMB and DHS charged with implementation and oversight of agency policies for security of government information
- NIST to develop the IT security standards
Types of Protected Information: Controlled Unclassified Information “CUI”

National Archives and Records Administration (NARA) has defined 22 Main Categories where information could be categorized as CUI.

- Agriculture
- Controlled Technical Information
- Copyright
- Critical Infrastructure
- Emergency Management
- Export Control
- Financial
- Foreign Government Information
- Geodetic Product Information
- Information Systems Vulnerability Information
- Intelligence
- Law Enforcement
- Legal
- NATO
- Nuclear
- Patent
- Privacy
- Proprietary Business Information
- SAFETY Act Information
- Statistical
- Tax
- Transportation

Information NOT Covered

Publicly available Information which would include information resulting from “fundamental research”
NIST 800-171

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

• 109 IT Security Controls!!!
• Ranging from password protection to physical security of IT devices
NIST 800-171
Example of Controls

3.10 PHYSICAL PROTECTION

Basic Security Requirements:

3.10.1 Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

3.10.2 Protect and monitor the physical facility and support infrastructure for those information systems.

Derived Security Requirements:

3.10.3 Escort visitors and monitor visitor activity.

3.10.4 Maintain audit logs of physical access.

3.10.5 Control and manage physical access devices.

3.10.6 Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites).
Where and how will it be implemented?

- Potentially in research contracts where researchers need to receive Controlled Unclassified Information
- Contract clause directly invoking NIST 800-171
- DFAR Clause 252.204-7012 (Sept 2015)
- FAR Clause scheduled to be released NLT 2016
Challenges for Research Institution

• Decentralized IT – no responsible individual
• Strict IT controls that could not be implemented at the enterprise level
• Most cloud services would not be compliant
• Will require additional IT assets and potentially physical security assets
Potential Solutions

• Refuse to receive CUI when possible

• Project-based compliance
  – Special Information Security plan specific to the project
  – Information access only at sponsor’s facility

• Centralized solution for project buy-in
  May require:
  – IT Consultant
  – Server
  – Security Officer for training and management
References

• FISMA Law:
  https://www.govtrack.us/congress/bills/113/s2521/text

• NIST 800-171:

• DFAR 252.204-7012