VirginiaTech
Invent the Future

New Process and Regulations for Controlled Unclassified Information

David Brady
TJ Beckett
Office of Export and Secure Research Compliance
http://www.oesrc.researchcompliance.vt.edu/

Agenda

- Background
- Identifying the issues
- Technical approaches and solutions

A Brief History of CUI:

The Approach

BACKGROUND

Virginia Tech
Invent the Future

Background: What is Controlled Unclassified Information?

Controlled Unclassified Information (CUI) is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

CUI Approach for Contractor Environment

Government

E.O. 13556

Registry

32 CFR 2002

NIST SP 800-171

FAR

Industry

1 Year

You are here.

Until the formal process of establishing a single FAR clause takes place, the CUI requirements in NIST SP 800-171 may be referenced in federal contracts consistent with federal law and regulatory requirements.

Where we are now

- CUI EO 13556 (November 4, 2010)
- CUI Registry established 2014-2015 (NARA Website)
- NIST 800-171 (June 2015, revised December 2016)
- DFAR 252.204-7012 latest revision (December 2015)
- FAR 52.204-21 (June 2016)
- DFAR 252.204-7000 (Oct 2016)
- 32 CFR 2002 (December 2016) Controlled Unclassified Information
- FAR Clause-proposed one year from issuance from of CFR
  - Federal Demonstration Partnership is working with FAR drafters
- NIST 800-171 full compliance in contracts with DFAR 7012 due date- December 31, 2017

Landscape

IT security requirements in agreements are increasing in frequency and scope

- Driving factors
  - data integrity and availability, standardization in data management, privacy, export controls, national security, economic espionage concerns

Data Breaches are the New Normal

Much of the discussion about data breaches focuses on the vulnerability of personal information (i.e. social security numbers, financial information, health records, etc…)

- This is Important!
- But, there is other sensitive information in the research university setting protected by contractual obligations, data use sharing agreements, regulation, and/or FARS or DFARS provisions

Our Unique Challenges

Decentralization means our institutional data protection policies are likely not uniformly followed across schools and departments

- One particular department or PI may adhere to certain policies, another department or PI may have completely different protocols.
- Having different standards internally:
  - will be cumbersome and confusing if and when there is a data breach
  - makes it difficult to comply with our varying contractual and legal obligations

Repercussions

What are the consequences of non-compliance?

- Lose your data
- Lose access for future research
- Cost and liability of breach
- Possible civil/criminal penalties (monetary fines)
- Research jeopardy

IDENTIFYING THE ISSUES

Federal Data Requirements

- Federal Information Security Modernization Act (**FISMA**)
- Controlled Unclassified Information (**CUI**) program - Established by Executive Order 13556
- Other

Federal Data Requirements

- Health Information Portability and Accountability Act (**HIPAA**)
- Federal Acquisition Regulation Basic Safeguarding of Covered Contractor Information Systems (June 2016)- **FAR 52.204-21**
- Defense Federal Acquisition Regulations (DFAR) - **DFAR 252.204-7012**
- Bureau of Labor Statistics (**BLS**) Security Provisions ,
- And more….

Federal Information Security Modernization Act of 2014 (FISMA)

- What is FISMA?
  - Requires federal agencies to strengthen information security programs and report progress back to Congress on an annual basis
- Why are we talking about FISMA?
  - FISMA is increasingly applied to federal contractors via terms of a federal contract or subcontract
  - Should be used only when your information system is connected to a USG FISMA compliant information system

Controlled Unclassified Information (CUI) Program

Defined by Executive Order 13556, published November 4, 2010

- Prior to EO 13556 more than 100 different markings for such information existed across the executive branch
- Ad hoc, agency-specific approach unnecessarily restricted information-sharing
- National Archives and Records Administration (NARA) is the Executive Agent for CUI
    - Create CUI Registry
    - Develop directives to implement CUI program (NIST 800-171)

NIST Special Publication 800-171

Defines IT security requirements for CUI residing on **nonfederal information systems.**

It is extremely challenging to comply with NIST 800-171 in many research settings.

- 110 active controls
- (DFAR) 7012 (December 2015) Safeguarding Covered Defense Information and Cyber Incident Reporting requires NIST 800-171 full compliance NLT December 31, 2017

NIST Special Publication 800-171

Defines IT security requirements for CUI residing on **nonfederal information systems.**

Coming soon:

- NARA will sponsor a single Federal Acquisition Regulation (FAR) clause that will apply the requirements in proposed CUI regulation and Special Publication 800-171 to contractors

- Department of Education has warned academia (July 2016) it intends to make student financial data subject to NIST 800-171controls, and to conduct a gap analysis between current security measures and NIST 800-171

CUI Marking

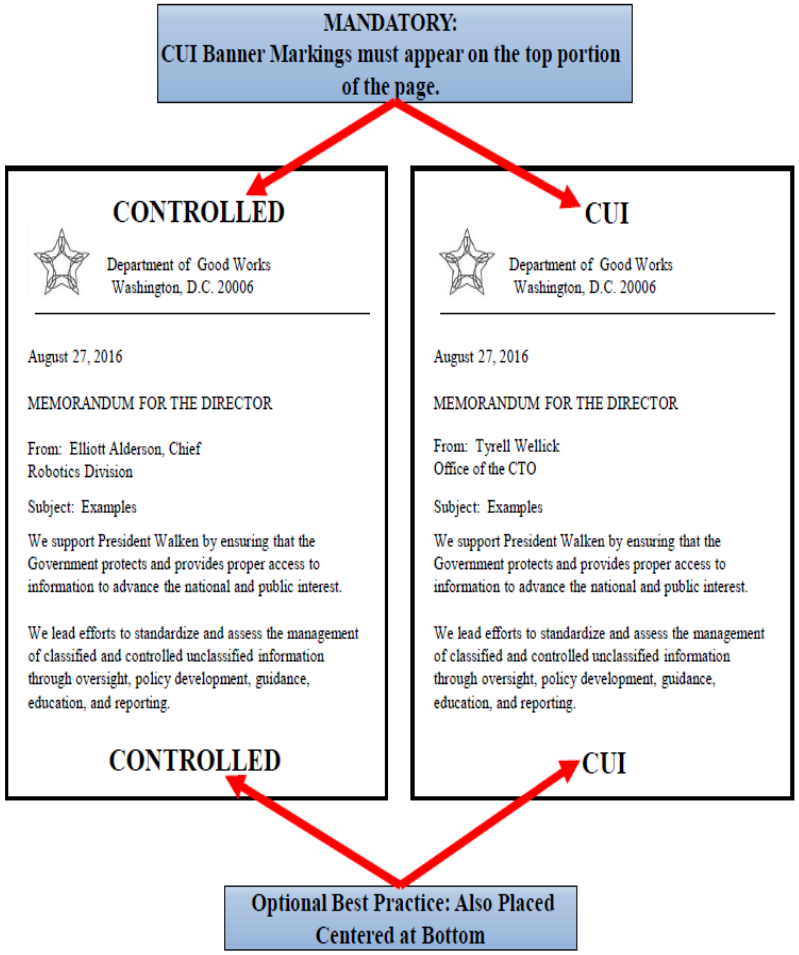
- 32 CFR 2002.15 Marking Requirements for USG
- Is extended to contractors by means of contract provisions
- USG responsible for marking CUI given to contractors
- “The implementation of this requirement is per CUI Marking Handbook Version 1.1 (NARA December 6, 2016)
  - CUI marking identified in category/subcategory (e.g., export control “EXPT” and “EXPTR”)

CUI Banner Markings (CUI Control Marking)

The CUI Control Marking is mandatory for all CUI and may consist of either the word "CONTROLLED" or the acronym "CUI" (at the designator's discretion).

As an optional best practice, the CUI Banner Marking may be placed at the bottom of the document as well.

Below are two examples showing the options for the CUI Banner Marking.



Reference: 32 CFR 2002.20(b)(1)

When do these restrictions become applicable?

- Information is described on NARA's list of categories and subcategories of CUI
  - Applies to CUI "Basic" only, not CUI "Specified"
  - CUI Specified- identified in legal citation under CUI category or subcategory

- There is a federal government nexus
  - Contract
  - Data Use Agreement

Research Agreements

What types of data do research agreements cover?

- Controlled Unclassified Information
  - Protected Critical Energy Infrastructure Information (PCII) (DHS)
  - Immigration information (legal status, asylee data)(DoS)
  - Export controlled information (DoS/DoC)
    - Controlled technical information
    - Covered defense information (DFAR 7012)
- Others….

Data Use Agreements (DUAs)

When are DUAs required?

Examples:

- Student financial data (DoE)
- Visa information-including Student Exchange Visitor Information System (SEVIS)(ICE)
- HIPAA-PHI (NIH/HHS)
- Export License Information (DoS/DoC)

Virginia Tech Timeline

Virginia Tech

- FY 2016-2017 University-wide senior level working group sponsored by VPs Research & Innovation and Information Technology
- Identifying academic and business units with CUI
- Identifying the gaps in security for CUI
- FY 2017/ 201818 Develop short, intermediate, and long term solutions

VirginiaTech
Invent the Future

TECHNICAL APPROACHES AND SOLUTIONS

VirginiaTech
Invent the Future

Compliant Environments

- **Considerations**: centralized vs. de-centralized, cost, buy-in
- **Options**:
- Cloud-based solutions
- Local enclaves
- Hybrid solutions

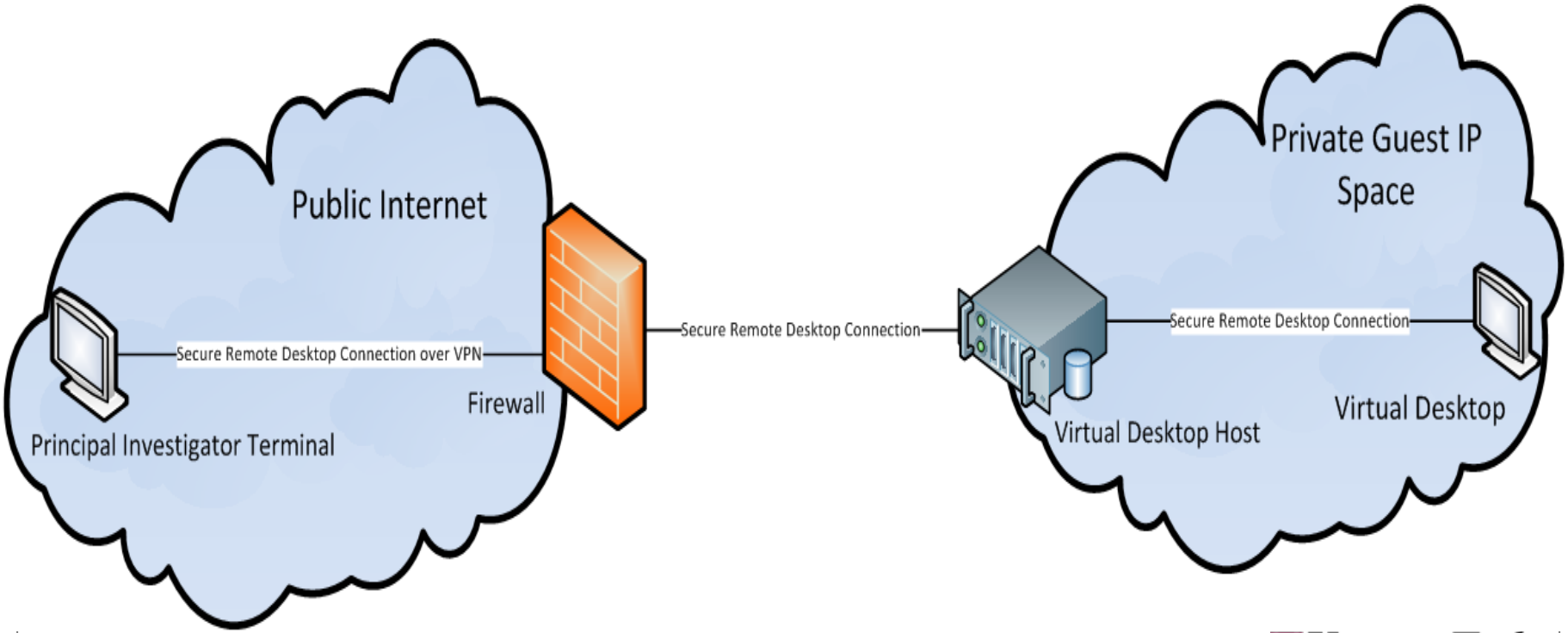
Compliant Environments

- **Cloud-based solutions**:
  - An environment hosted by an external provider (e.g. Amazon Gov Cloud, Google Government)
- **Pros and Cons**:
- Alleviates the need for on-site managed hardware
- Can scale easily to demand
- Redundancy for service availability and data recovery are the highest priorities.
- Attestation that systems have met all compliance standards can be hard to obtain.
- Flexibility for changing user demands is difficult.
- Connection to peripheral devices problematic.
- Cost depends on user base and needs.

Compliant Environments

- **Enclave solutions**:
  - The entire environment is hosted on-site
- **Pros and Cons**:
  - Can be more expensive, especially when redundancy requirements are factored in
  - Scaling to user demand more difficult unless excess capacity already exists
  - All compliance requirements must be implemented locally.
  - Connection to peripheral devices problematic.
  - Solutions are more traditional and often more familiar to local IT staff
    - Especially for some security requirements

VT Secure Research Enclave Environment



Compliant Environments

- **Hybrid solutions**:
  - A local solution that combines the local enclave with individual workstations where information is stored and processed.
- **Pros and Cons**:
- Requires purchasing equipment
- Scaling can be costly due to hardware costs.
- Redundancy for service availability and data recovery are dependent on local staffing and equipment availability.
- Compliance is monitored locally but can be demanding since compliance is required on de-centralized workstations.
- Flexibility is the highest.

Roles and Responsibilities

- Principal Investigator
- Departmental Information Technology Administrator
- Collaborative Computing Solutions
- IT Security
- Security Management Office
- Sponsored Programs
- Legal Counsel
- Bursar
- Others

Resources

- An Introduction to NIST Special Publication 800-171 for Higher Education Institutions (Educause)

https://library.educause.edu/~/media/files/library/2016/4/nist800.pdf

Office of Export and Secure Research Compliance
CONTACT US!

www.oesrc.researchcompliance.vt.edu; oesrc@vt.edu

David Brady

Director/ FSO

540-231-3801 dbrady@vt.edu

Export and Sanctions Policies and Procedures, Export and Sanctions Regulatory Reviews and Responses, Facility and Industrial Security, International collaborations, technology issues- chemical, biological, and Select Agents, International Visitors and Visas, General Export and Sanctions Training

Mike Kendrick

Export and Secure Research Program Manager

540-231-6902 mkendric@vt.edu

Export and Sanctions Determinations in Sponsored Research, Export Licensing and Technical Assistance Agreements, International Collaborations, International Visitors and Visas, CDA and MTA Export and Sanctions reviews, General Export and Restricted Research Training

Tom Czamanske

Export and Secure Research Administrator

540-231-5878 tczamanske@vt.edu

Export and Sanctions Determinations in Sponsored Research, Export Licensing and Technical Assistance Agreements, International Visitors and Visas, International Shipping, DoE/NRC Export Regulations

Amanda Gland

Admin. Specialist

540-231-6642 agland@vt.edu

Travel Information and Advisories, Training Information/Scheduling, Restricted Party Screening, Database and Records Management

Security Management Office CONTACT US!

smo@vt.edu

John Talerico
Export and Secure Research Program Manager/Deputy Facility Security Officer
540-231-6583 jtaleric@vt.edu

Research Security, Technology Control Plans, Restricted Research Training, Post Award Monitoring

TJ Beckett
Information Security Compliance Officer
540-231-9230 beckett@vt.edu

Information Security, Technology Control Plan IT Officer

Melissa Leake
Assistant Facility Security Officer/Data Entry Technician
540-553-3951 nlittier@vt.edu

Industrial Security, Visit Requests, Document Control