SAN DIEGO STATE UNIVERSITY
Research Foundation

National Institute of Standards and Technology (NIST 800-171) Has Arrived: Have You?

Sandra M. Nordahl, CRA
Director, SR Contracting and Compliance
and
Facility Security Officer

What is NIST 800-171

Implementation date no later than December 31, 2017!

- Majority of requirements are related to policy, process and configuring IT securely
- Statutory mandate as part of the Federal Information Security Modernization Act (FISMA) of 2014
- Requirements were derived from FIPS Publication 200, “Minimum Security Requirements for Federal Information and Information Systems” based on regulation in 32 CFR Part 2002, Controlled Unclassified Information.
- Mapping Table is provided in Appendix D
  - Maps each requirement to relevant security controls


Don’t feel like a fish out of water…

Key Points

- Provides requirements when physical or verbal information that is classified as Controlled Unclassified Information (CUI) and Controlled Defense Information (CDI) resides outside of the U.S. federal control.
- Provides requirements for information systems (e.g. computers, hand held devices, shared networks) when CUI/CDI resides outside of U.S. federal systems/control.
- When project/activity is determined after award to involve CUI/CDI in the project/activity (e.g. Christian doctrine).

When Does NIST 800-171 affect your institution?

- Key words
  - Safeguarding of information required
  - Prior approval to disseminate/publish required
  - Controlled Defense Information (CDI)
  - Controlled Unclassified Information (CUI)
- Activities
  - Financial aid
  - Student records
  - Sponsored programs
- Institution has the ultimate responsibility for implementation
  - 3rd party assessments are not authorized or recognized

FAR and DFAR clauses related to CUI/CDI

- 52.204-21: Compliance with Safeguarding Covered Defense Information Controls
- 252.204-7000: Disclosure of Information
- 252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting

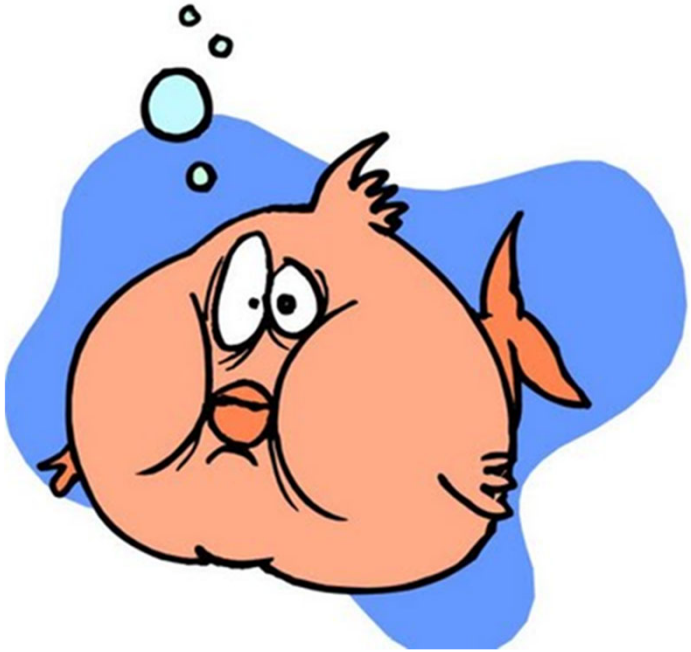
52.204-21: Basic Safeguarding of Covered Contractor Information Systems

- Applies to any system that processes, stores or transmits federal information that is not intended for public release.
- Information provided by or generated for the Federal government.
  - under a contract or subagreement
  - provides minimum basic safeguarding requirements
- Three prime provisions:
  - Definitions
  - Minimum safeguarding requirements and procedures
  - Flow down provisions

252.204-7000: Disclosure of Information

- **NO** release of information unless:
  - Prior written approval
    - Requires request to release be made at least 10 business days prior proposed release date
      - Identify medium, specific information to be released and purpose of release.
  - Information is already in the public domain
  - Project involves NO covered defense information AND determined in writing to be fundamental research
- Flow down of similar provision in all subcontracts is required.

252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting



The Condensed Definitions of 252.204-7012

- Adequate security”
  - protective measures
  - commensurate with the consequences and probability of loss, misuse, or unauthorized access

- “Compromise” means
  - disclosure of information to unauthorized persons
  - violation of the security policy of a system
  - unauthorized intentional or unintentional disclosure
  - modification, destruction, or loss of an object, or copying of information to unauthorized media

Definitions continued…

- Contractor attributional/proprietary information”
  - information that identifies the contractor
  - personally identifiable information
  - trade secrets, commercial or financial information, or other commercially sensitive information
  - not customarily shared outside of the company

- “Technical information”
  - technical data or computer software
    - e.g. research and engineering data, drawings, specifications, process sheets/manuals, technical reports/orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software code.

Definitions continued…

- Controlled technical information”
  - technical information with military or space application
  - subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.
  - distribution statements B through F (Distribution Statements on Technical Documents).

- “Covered contractor information system”
  - unclassified information system
  - owned, or operated by or for, a contractor
  - processes, stores, or transmits covered defense information.

Definitions continued…

- "Covered defense information"
  - described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html
    - marked or otherwise identified in the contract,
    - provided to the contractor by or on behalf of DoD in support of the performance of the scope of work;
    - information (all forms) collected, developed, received, transmitted, used, or stored by entities' personnel.

Definitions continued…

- "Cyber incident" is an intrusion, disruption, or other event that impairs the integrity or availability of electronic systems.
- "Malicious software" software or firmware which performs unauthorized process(es) that will have adverse impact on an information system.
  - e.g.: virus, worm, Trojan horse, or spyware and some forms of adware.
- "Rapidly report" means within 72 hours of discovery of any cyber incident at: http://dibnet.dod.mil


Too much information !!!

252.204-7012: Prime Recipient Requirements

- IT service or system operated on behalf of the federal government.
- Covered contractor information systems that are NOT part of an IT service/system operated on behalf of the federal government.
  - Implements NIST 800-171
  - Must notify DoD Chief Information Officer (CIO) within 30 days of award, if not in compliance with NIST requirements.
- Flow down if determined that subrecipient will:
  - Provide "operationally critical support" OR
  - Involves CDI

252.204-7012: Subrecipient Requirements

- Notify Prime to request variance from NIST security requirements
- When reporting cyber incidents to DoD must provide incident number to the prime (or next higher tier subcontractor).

NIST Special Publication 800-171

- Compliance is challenging
  - Not just sponsored programs activities
    - Crosses many areas of organizations
  - Recommendations, not mandates for compliance
    - Non compliance may affect ability to receive certain awards
  - Requires outreach to ensure compliance

What are the requirements?

- Training
- Physical and verbal protection of information
- Limitation of access to organizational information systems, equipment and/or operating environments to only authorized individuals
- Escorting/monitoring of visitors within the “controlled” environment
- Control and management of physical access to “controlled” devices/information
- Technology Control Plan
- Recognizing and reporting potential indicators of insider threats


OH, NO
HELP
ME!!!

CUI Definitions, Regulations and Negotiations

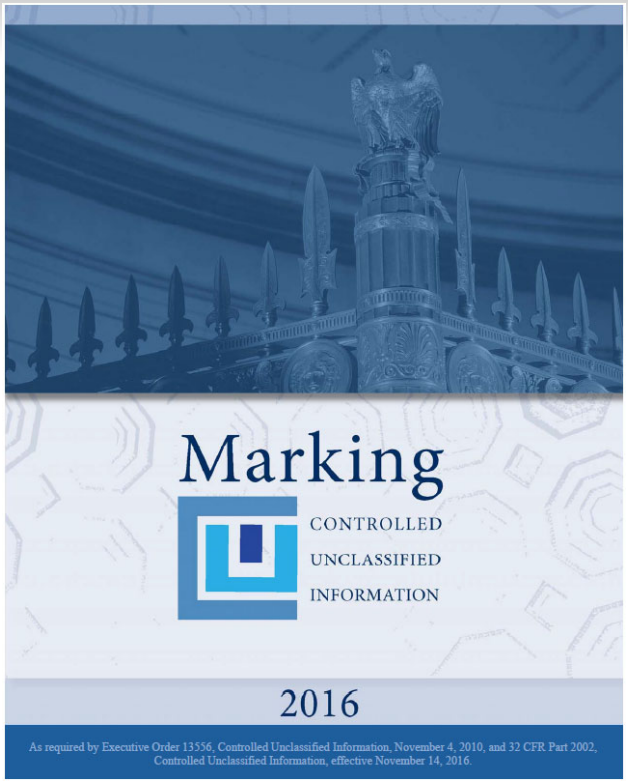
- Why CUI?
  - Implemented to
    - Create uniform treatment of information that requires "safeguarding or dissemination controls"
    - Addresses inefficiency and inconsistencies in marking and safeguarding policies and procedures
- What is CUI?
  - Information created/possessed by
    - Government and/or sponsor
    - Organization's project director and/or staff

Common Categories of CUI Subsets

- Agriculture
- Critical Infrastructure
- Emergency Management
- Export Control
- Financial
- Geodetic Product Information
- Immigration
- Information Systems Vulnerability Information
- Intelligence
- International Agreements
- Law Enforcement
- Legal
- Natural and Cultural Resources
- NATO Controlled
- Nuclear
- Patent
- Privacy
- Procurement and Acquisition
- Proprietary Business Information
- SAFETY Act Information
- Statistical
- Tax
- Transportation

CUI "Markings"

- Marking requirements found in the "Marking Controlled Unclassified Information" handbook: https://fas.org/sgp/cui/marking-2016.pdf



What do CUI "Markings" look like?

Banner Marking

Use the Limited Dissemination Control Markings found on the CUI Registry (*www.archives.gov/cui/*).

Limited Dissemination Control Markings

CUI//SP-SPECIFIED//DISSEMINATION

Department of Good Works
Washington, D.C. 20006

August 27, 2016

MEMORANDUM FOR THE DIRECTOR

From: John E. Doe, Chief Division 5

Subject: Examples

We support the President by ensuring that the Government protects and provides proper access to information to advance the national and public interest.

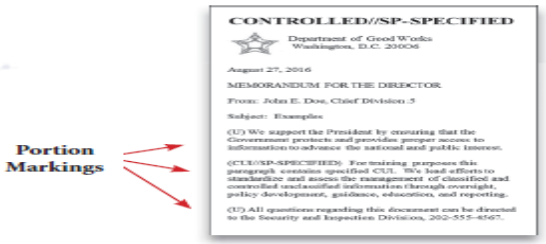
We lead efforts to standardize and assess the management of classified and controlled unclassified information through oversight, policy development, guidance, education, and reporting.

NOTE: The above example uses the word "DISSEMI-NATION" as a substitute for a Limited Dissemination Control Marking. See the CUI Registry for actual markings.

Portion Marking

- Portion marking is permitted and encouraged to facilitate information sharing and proper handling of the information. When used, the abbreviations, in parentheses, are placed at the beginning of the portion to which they apply and throughout the entire document.
- Using portion markings may be optional (or required in agency policy), but when using them, follow these rules.
- CUI portion markings may include up to three elements:
  - The CUI Control Marking (the acronym "CUI").
  - CUI Category or Subcategory Markings (mandatory for CUI Specified).
  - Limited Dissemination Control Markings.
- When portion markings are used and a portion does not contain CUI, a "U" is placed in parentheses to indicate that the portion contains unclassified information.

Portion Markings



Portion Marking up close

CONTROLLED//SP-SPECIFIED

Department of Good Works
Washington, D.C. 20006

August 27, 2016

MEMORANDUM FOR THE DIRECTOR

From: John E. Doe, Chief Division 5

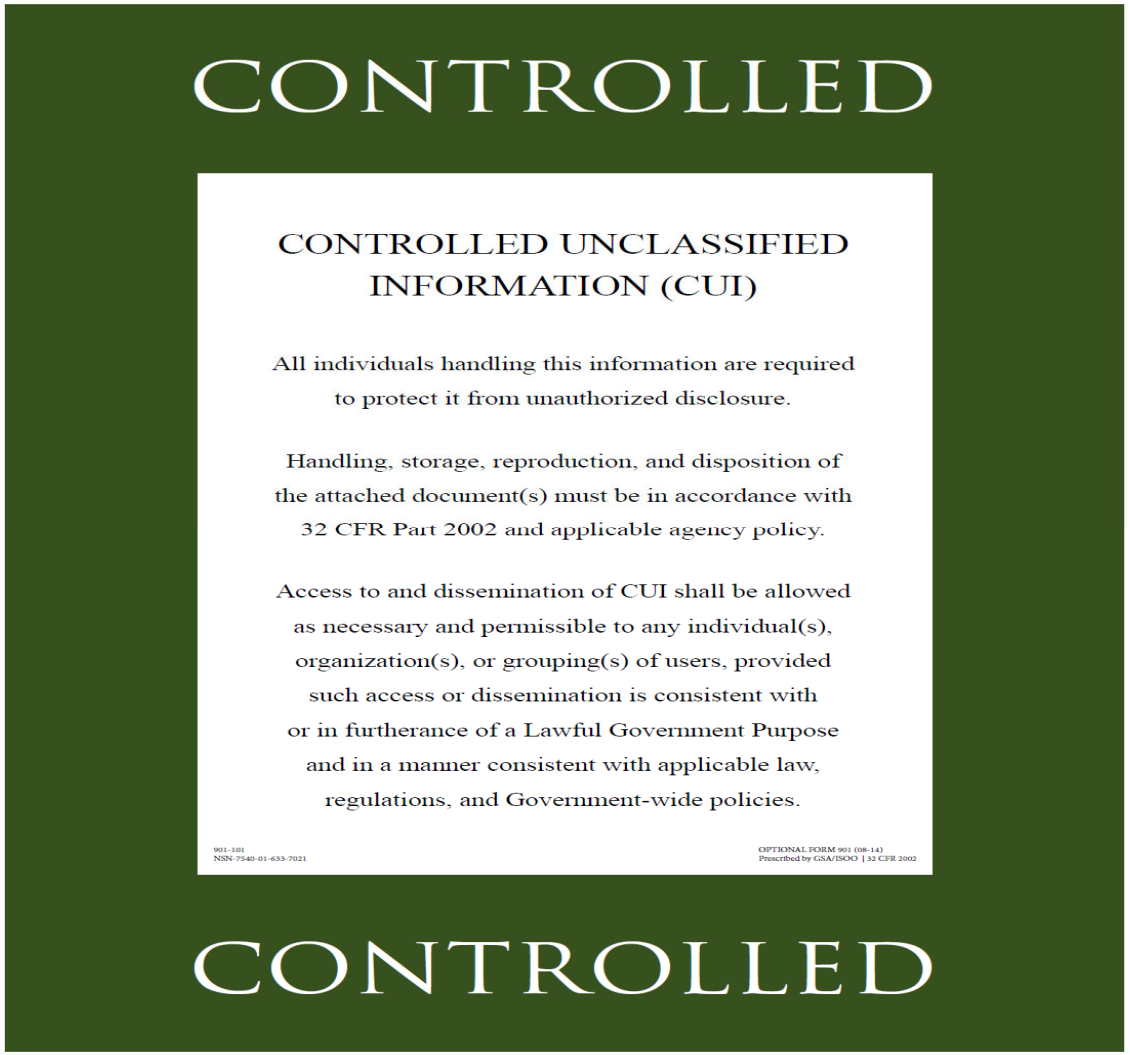
Subject: Examples

(U) We support the President by ensuring that the Government protects and provides proper access to information to advance the national and public interest.

(CUI//SP-SPECIFIED) For training purposes this paragraph contains specified CUI. We lead efforts to standardize and assess the management of classified and controlled unclassified information through oversight, policy development, guidance, education, and reporting.

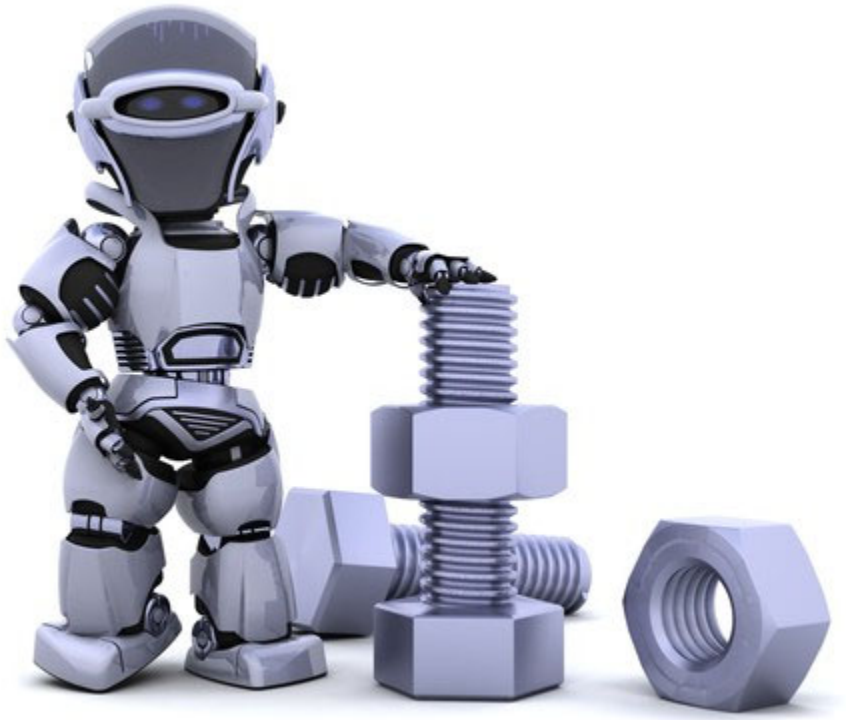
(U) All questions regarding this document can be directed to the Security and Inspection Division, 202-555-4567.

Cover Page for Controlled Unclassified Information



Equipment labels for approved equipment to destroy CUI materials

Now for the Nuts and Bolts!



Implementation of NIST 800-171

- Started with a simple conversation
- Shared materials provided jump point
- Determined stakeholders
  - Information and Technology Security Officer (ITSO)
    - If applicable, college/department ITSOs
  - Export Control Officer
  - Sponsored Programs
  - Other areas to consider (HIPPA, FERPA, FISMA, etc.)
    - Financial Affairs
    - Student Affairs
    - Any other area that may have sensitive information covered by NIST 800-171

First "To Do List"

- **BREATHE!**
  - Schedule meetings
  - Review matrix
    - Determine stakeholders and roles
      - Policy, technical or both
  - Draft policy/procedures documents
  - Send annotated copies of NIST 800-171 and matrix to appropriate individuals
  - Update policies and procedures
  - Draft communication to appropriate individuals
  - Draft flow charts
  - Determine who pays

Next Action List…

- Determine the roles/responsibilities of the stakeholders
  - Owners (end user)
  - Custodians (use data)
  - Campus Managers
  - Sponsor
  - Compliance team (Export Control/Sponsored Programs)
- Create general policy statement
- Sponsored programs education plan
  - Project directors
  - Chairs and Deans
  - ITSO
  - Sponsored Programs

Feeling… stressed, incompetent, stunned, dazed, confused, overwhelmed, exhausted, incapable, worried, strained, hassled, frazzled, bewildered, confounded, baffled, bewildered???

Try Yoga!!!

Work the grid…

- Determine which stakeholder was relevant for each item:
  - End User (department/project personnel)
  - Export Control
  - Human Resources
  - IT
  - Sponsored Programs
  - Web provider (cloud services)
- Determine if item is:
  - Policy
  - Technical
  - Or…Both

Table D-1: Mapping Access Control Requirements to Security Controls

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.1 ACCESS CONTROL				
Basic Security Requirements				
3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems). 3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.	AC-2	Account Management	A.9.2.1	User registration and de-registration
			A.9.2.2	User access provisioning
			A.9.2.3	Management of privileged access rights
			A.9.2.5	Review of user access rights
			A.9.2.6	Removal or adjustment of access rights
	AC-3	Access Enforcement	A.6.2.2	Teleworking
			A.9.1.2	Access to networks and network services
			A.9.4.1	Information access restriction
			A.9.4.4	Use of privileged utility programs
			A.9.4.5	Access control to program source code
			A.13.1.1	Network controls
			A.14.1.2	Securing application services on public networks
			A.14.1.3	Protecting application services transactions
			A.18.1.3	Protection of records
	AC-17	Remote Access	A.6.2.1	Mobile device policy
			A.6.2.2	Teleworking
			A.13.1.1	Network controls
			A.13.2.1	Information transfer policies and procedures
			A.14.1.2	Securing application services on public networks

More detailed processes

- Detailed by area within the grid
  - Access Control
  - Awareness & Training
  - Audit & Accountability
  - Configuration Management
  - Identification & Authentication
  - Incident Response
  - Maintenance
  - Media Protection
  - Personnel Security
  - Physical Protection
  - Risk Assessment
  - Security Assessment
  - System & Communication Protection
  - System & Information Integrity

Table D-1: Mapping Access Control Requirements to Security Controls

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.1 ACCESS CONTROL				
Basic Security Requirements				
3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems). 3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.	AC-2	Account Management	A.9.2.1	User registration and de-registration
			A.9.2.2	User access provisioning
			A.9.2.3	Management of privileged access rights
			A.9.2.5	Review of user access rights
			A.9.2.6	Removal or adjustment of access rights

Tips for drafting a policy statement

- Keep it simple
- Added to existing Data Classification and Handling Policies:

  "In addition to minimum standards, additional requirements may apply to specific awards. PIs, project directors and staff are responsible for compliance with regulations which include, but are not limited to handling of Controlled Unclassified Information, Covered Defense Information and Export Controlled Information. More information regarding these requirements can be found at:

  - Federal Acquisition Regulations (FAR) 52-204.21: Basic Safeguarding of Covered Contractor information Systems (http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/far/52_000.htm#P889_130330)
  - Defense Federal Acquisition Regulation (DFAR) 252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting (https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012
  - CUI Registry – Categories and Subcategories (https://www.archives.gov/cui/registry/category-list)
  - NIST 800-171: Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations (https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/archive/2016-12-20)"

IT Solutions

- Determine who has purview of the “controlled systems”
- Work with ITSO and relevant IT groups
  - Developed plan for implementation when CUI/CDI is present
    - Includes cloud based web services that **<u>are complaint</u>**
    - May also include “developed” systems that meet requirements
  - When appropriate, budget for specialized services
    - Ensure that costs are treated the same
      (Uniform Guidance §200.412 Classification of costs

Education is the Key…

- Communicate directly with affected project personnel
- Conduct outreach
  - Tailor to meet the needs of the audience
    - Short
    - Simple
  - In person meetings
  - Workshops
    - Project personnel meetings
    - Sponsored Programs

Naysayers…

- Ostrich philosophy doesn't work.
- Need to have a way to embargo until compliance is achieved.
- Two-way communication is a must.


ONWARD…CHARGE!

At the proposal stage…

- Now part of the application process
  - Describe compliance with NIST 800-171
    - See Sections L and M of solicitation
      - Describe plan for compliance and implementation
  - Separate from DFARS 252.204-7012 compliance description
  - Source Selection Plan, if applicable will be an evaluation factor
    - Sponsor will determine if risk is acceptable or unacceptable to process, store or transmit CDI/CUI on a system hosted by the offeror.
- Must be implemented at time of award

Upon receipt of an award…

- Identify any CDI/CUI that is provided by the sponsor
- Communication critical!
  - Determine if Scope of work is fundamental research
  - Work with the Export Control Officer to implement a Technology Control Plan (TCP), if needed.
    - TCP will include:
      - What is the CDI/CUI?
      - Who possesses/has access to the CDI/CUI?
      - Where is the CDI/CUI stored?
- Work with the IT representative to ensure proper safeguarding of information

CUI and Export Controls in Research Agreements

- May negate Fundamental Research Exemption (FRE)
  - Control plans can be put in place to mitigate risk
- Negotiation approach will depend on institutional **and** individual circumstances
  - No “one-size fits all” solution

The Good News…

- If no CUI/CDI:
  - Council on Governmental Regulations (COGR) re-confirmed at the October 2017 that clauses are “self-deleting.”
  - Request waiver from the sponsor

DFAR 7000 and DFAR 7012 Relief

Request waiver if:

- Project does not involve any covered defense information as defined in 252.204-7012
- Confirm with project director and programmatic officer that the scope of work is fundamental research
- Write letter to contracting officer requesting relief

Drafting a Relief Request

- Who
  - If prime – request directly from Contracting Officer
  - If subrecipient – request from Prime
- Why
  - Fundamental Research – Yes or No
  - Explain how the scope of work does not meet CDI/CUI requirements
  - Publication expectations = YES
- Reference
  - DoD Directive 189
  - Secretary of Defense Memorandum - May 24, 2010


I CAN SEE CLEARLY NOW…

DoD Directive 189

Key Point One:
Defines federally funded fundamental research

THE WHITE HOUSE

WASHINGTON

September 21, 1985

NATIONAL SECURITY DECISION

DIRECTIVE 189

NATIONAL POLICY ON THE TRANSFER OF SCIENTIFIC, TECHNICAL AND ENGINEERING INFORMATION

I. PURPOSE

This directive establishes national policy for controlling the flow of science, technology and engineering information produced in federally funded fundamental research at colleges, universities, and laboratories. Fundamental research is defined as follows:

"'Fundamental research' means basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons."

DoD Directive 189 continued

Key Point Two:

Work to remain unrestricted

III. POLICY

It is the policy of this Administration that, to the maximum extent possible, the products of fundamental research remain unrestricted. It is also the policy of this Administration that, where the national security requires control, the mechanism for control of information generated during federally funded fundamental research in science, technology and engineering at colleges, universities and laboratories is classification. Each federal government agency is responsible for: a) determining whether classification is appropriate prior to the award of a research grant, contract, or cooperative agreement and, if so, controlling the research results through standard classification procedures; b) periodically reviewing all research grants, contracts or cooperative agreements for potential classification. No restriction may be placed upon the conduct or reporting of federally funded fundament research that has not received national security classification, except as provided in applicable U.S. Statutes.

Secretary of Defense Memorandum May 24, 2010

- Reiterates results of fundamental research should not be restricted
- Compliance with NSDD 189
- Applies to grants and contracts

THE UNDER SECRETARY OF DEFENSE
3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

ACQUISITION, TECHNOLOGY AND LOGISTICS

MAY 24 2010

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
ATTN: SERVICE ACQUISITION EXECUTIVES
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
ATTN: COMMANDER, U.S. SPECIAL OPERATIONS COMMAND
DIRECTORS OF THE DEFENSE AGENCIES

SUBJECT: Fundamental Research

References: (a) DoD Directive 5230.24, "Distribution Statements on Technical Documents," March 18, 1987
(b) DoD Instruction 5230.27, "Presentation of DoD-Related Scientific and Technical Papers at Meetings," October 6, 1987

The Department of Defense (DoD) fully supports free scientific exchanges and dissemination of research results to the maximum extent possible. Critical to enabling exchanges and dissemination is an understanding on the part of DoD acquisition personnel and the research community of the statutes, regulations, and policies governing restrictions that apply to the DoD on basic and applied research, recognizing the necessarily open nature of unclassified fundamental research. Understanding will help guide DoD acquisition personnel and contract and grant recipients in making plans and decisions that will affect performance of research under DoD awards and implementing measures that may be needed to comply with appropriate controls.

I have determined that additional clarifying guidance is required to ensure the DoD will not restrict disclosure of the results of fundamental research, as herein defined, unless such research efforts are classified for reasons of national security or as otherwise required by applicable federal statutes, regulations, or executive orders. This memorandum reinforces earlier guidance (Attachment A), addresses residual issues, and deals explicitly with additional facets of fundamental research. My intention is to ensure that the DoD grants, contracts, and negotiations with the research community for fundamental research are consistent across Components and fully compliant with National Security Decision Directive (NSDD) 189 (Attachment B).

Excerpt from page 2…

NSDD 189 makes clear that the products of fundamental research are to remain unrestricted to the maximum extent possible. When control is necessary for national security reasons, classification is the only appropriate mechanism. The DoD will place no other restrictions on the conduct or reporting of unclassified fundamental research, except as otherwise required by applicable federal statutes, regulations, or executive orders.

May 24th Memorandum: Contracted Fundamental Research

The definition of "contracted fundamental research" in a DoD grant or contractual context is established by References (a) and (b) and is defined as follows:

> "'Contracted Fundamental Research' includes research performed under grants and contracts that are (a) funded by budget Category 6.1 ("Research"), whether performed by universities or industry or (b) funded by budget Category 6.2 ("Exploratory Development") and performed on-campus at a university. The research shall not be considered fundamental in those rare and exceptional circumstances where the 6.2-funded effort presents a high likelihood of disclosing performance characteristics of military systems or manufacturing technologies that are unique and critical to defense, and where agreement on restrictions have been recorded in the contract or grant."

Defense Related FRE request

Dear XXXXXXXX,

This letter is being submitted on behalf of insert Your Organization's Name and Dr. Your Project Director to formally request a waiver of the insert cite of language to be removed from document, which also restricts the insert restriction listed in document for the Subaward XXX-XXXXXX-XX-X-XXXX-XXXX.

The proposed work to be performed is fundamental research on the insert nature of the work to be performed. The project does not emphasize any chosen special material for specified applications. Dr. XXXXXXX's work will focus on insert emphasis of work to be performed. No hardware or software will be developed as a result of the research. Dr. XXXXXXX does not anticipate the need to work with any covered defense information, data, hardware or software. Nor will any covered defense information, data, hardware or software be received from insert sponsor name or the government sponsor to complete the scope of work as outlined in the Subaward. Dr. XXXXXXX does not anticipate generating any covered defense information, data, hardware or software during the project period of the Subaward. As provided by if applicable, cite where publications are allowable, Dr. XXXXXXX fully intends to publish the progress and results of the work. Further, as an academic institution work is conducted with a vast array of students, including non-US citizens.

After careful review and consideration, the Export Control Officer, Ms. XXXXXXX and Dr. XXXXXXX consider this project to be fundamental research, as outlined in the DoD Directive 189, dated September 21, 1985 and explained in the Secretary of Defense Memorandum dated May 24, 2010. The Secretary of Defense Memorandum dated May 24, 2010 further states, "The DoD will place no other restrictions on the conduct or reporting of unclassified fundamental research, except as otherwise required by applicable federal statutes, regulations, or executive orders."

In accordance with the Secretary of Defense's memorandum **and because the Subaward is not marked as restricted for proprietary or national security reasons**," SDSU Foundation respectfully requests that the restrictive language in Article XX be removed.

Please do not hesitate to contact me, should you have questions or require additional information.

Best Regards,

Sandra M. Nordahl, CRA
Director, Sponsored Research Contracting and Compliance

Attachments: National Security Directive 189
DoD Fundamental Research Memorandum 5-24-2010


Prepare
Yourself…
An AUDIT
is coming…

Just a little email…

Hello Lance and Sandra,

XXXX received a request from our client at the Department of the Navy (DoN), Space and Naval Warfare Systems Command (SPAWAR) that we, along with all of our active subcontractors on this program, must provide certification of our compliance to the Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting.

In response to this request, we are asking our subcontractors to provide to XXXX the same certification of your compliance with the subject clause to include, at minimum, a reference to any substantiating documentation you have to support your self-attestation to meeting the requirements of DFARS Clause 252.204-7012. Such substantiating documentation may include, but are not limited to, a System Security Plan (SSP).

Your reply is requested no later than **4PM PST Friday, September 28, 2018. Please confirm receipt of this email, and indicate your company's ability to meet the deadline**. Should you have any questions or concerns, please do not hesitate to reach out. Your prompt attention is appreciated.

If you have any questions or concerns please contact me at the number below or XXXX Contracts Dept. at Contracts@xxxx.com. Thank you.

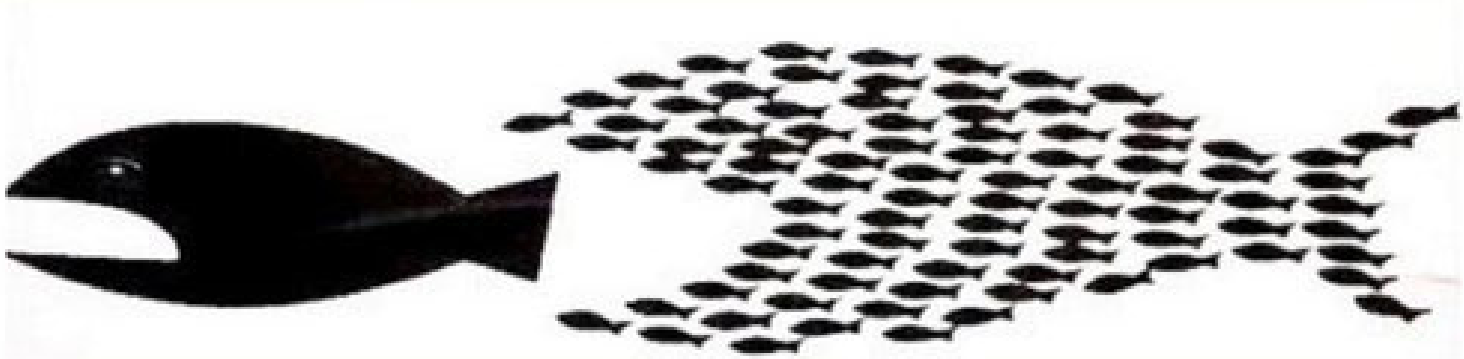
Very Respectfully,

Sheila

Just a little internal audit recommendation…

- **Recommendations to Management:**
- Develop a detailed plan of action and milestones (POA&M) to implement the interim approach for compliance of OU Research grants and contracts subject to a DFARS 252.204-7012 clause. The plan should
  - Identify
    - Specific tasks needing to be accomplished, including the development of needed capabilities and the establishment and execution of needed processes, functions, and activities.
    - Resources required for the implementation and maintenance of all required elements of the plan, including human, technology, service, and financial resources.
    - Providers of the above identified required resources.
    - Roles and responsibilities for the implementation and maintenance of all required elements of the plan/program/strategy.
    - Milestones and respective completion dates for key phases and tasks of the plan.
  - Document agreement of all involved parties with respect to
    - Assigned roles and responsibilities.
    - Providers of the needed resources.
  - Establish processes for
    - Periodic re-assessment to determine if the current approach continues to adequately address the compliance, efficiency, and economic objectives of OU Research.
    - Ongoing oversight of technical compliance for CUI to determine whether the controls in place are effective in their application.
  - Be approved by appropriate OU Research leadership, including the Vice President for Research, the Vice President & Chief Information Officer, the Senior Vice President and Provost, and Vice President & General Counsel.
- Determine a strategy and plan of action for OU Research to monitor and respond to evolving compliance requirements of U.S. federal government executive agencies for Controlled Unclassified Information.
  - The plan should consider strategic synergies of common infrastructure and processes, including efficiencies and consistency.

DON'T PANIC



ORGANIZE!

Assess projects

- Maintain a list of projects with applicable clauses
  - Start/end dates
  - PI
  - On/off campus
  - Training materials provided/accomplished
- Ensure that policy/procedures are updated

Compilation of Documentation

- Determine systems accessed
  - On campus v. off campus
  - Work with relevant departments (ITSOs) to ensure that systems are in compliance
    - Ask for documentation
- Ask for training certifications for required trainings
- Include staff training

Documentation organization

Document Name/Title	Doc Type	Doc Number	Version/Rev	Date
SAN DIEGO STATE UNIVERSITY RESEARCH FOUNDATION (SDSURF)	SDSU Research foundation conducts **ALL** classified contracts off campus and **ONLY** at cleared USER AGENCY sites or PRIME Agency locations. **NO** classified work or access takes place on the premises of San Diego State University or San Diego State University Research Foundation. No data is processed, stored or transmitted on San Diego State University /San Diego State University Research Foundation systems.			
SDSURF Research Foundation Data Classification and Handling Policies	Policy	ix. – Section 3.0, http://security.sdsu.edu/policy		12/2017
Training: Counterintelligence Awareness and Security Brief;	Training	N/A	N/A	05/24/18
Training: Cyber Awareness Challenge – Intelligence Community	Training	N/A	N/A	09/10/18
Training: Derivative Classification	Training	N/A	N/A	09/07/18
Training: Identifying and Safeguarding Personally Identifiable Information (PII)	Training	N/A	N/A	09/10/18
Training: Insider Threat Awareness	Training	N/A	N/A	05/24/18

Training: Understanding and Complying with NIST 800-171: How does it affect you?
Understanding the Process…This workshop discusses:
• An overview of protected information
• Determining affected projects and activities
• Examples of access controls and requirements mandated
• Review of FAR/DFAR clauses:
  ○ 52.204-21
  ○ 252.204-7000
  ○ 252-204-7012
  ○ 252-225-7048
  ○ 2523239-7999
	Training	N/A	N/A	09/25/18

Documentation organization

- Project Administration Guide
- 800-171 GAP Assessment and Tasks
- Virtual “Notebook” on each CUI project
  - TCP
  - Consistency is key
  - Project specific when needed

Response Example

September 25, 2018

Ms. Sheila
XXXX, Inc.
XXXXXXXXXXXX
San Diego, CA 92XXX

Subject: Notice Regarding Compliance/Non-Compliance with DFARS 252.204-7012

Dear Ms. Sheila:

San Diego State University Research Foundation hereby verifies compliance with DFARS Clause 252.204-7012.

I hereby confirm the statement made above is true and accurate to the best of my knowledge.

Signed,

Sandra M. Nordahl, CRA
Director of Contracting and Compliance
and Facility Security Officer

Substantiating Documentation

- SDSU Research Foundation Data Classification and Handling Policies (attached)
- SDSU Research Foundation conducts **ALL** classified contracts off campus and **ONLY** at cleared USER AGENCY sites or PRIME Agency locations. **NO** classified work or access takes place on the premises of San Diego State University or San Diego State University Research Foundation. No data is processed, stored or transmitted on San Diego State University/San Diego State University Research Foundation systems. As such, Dr. XX has conducted work only at authorized facilities using only U.S. Navy infrastructure and architecture.

Additional training related to this contract includes:

- Counterintelligence Awareness and Security Brief
- Cyber Awareness Challenge – Intelligence Community
- Derivative Classification
- Identifying and Safeguarding Personally Identifiable Information (PII)
- Insider Threat Awareness
- Understanding and Complying with NIST 800-171: How does it affect you? Understanding the process…

Further, individuals who receive funding with any of the above referenced clauses discuss their project in depth with the SDSU Export Control Officer. A Technology Control Plan is developed to meet the individual needs of each project.

Resource Tools

https://www.archives.gov/cui/training.html

- Website has training videos related to:
  - Controlled Environments
  - Decontrolling
  - Destruction requirements
  - Introduction to Marking
  - Marking: Non-Traditional
  - Unauthorized Disclosures: Preventing and Reporting

Resources: Overview

- Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, SP 800-171 Rev.1
  https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/archive/2016-12-20
- An Introduction to NIST Special Publication 800-171 for Higher Education Institutions
  http://library.educause.edu/~/media/files/library/2016/4/nist800.pdf
- About Controlled Unclassified Information (CUI)
  https://www.archives.gov/cui/about
- CUI Registry: Categories and Subcategories
  https://www.archives.gov/cui/registry/category-list
- CUI Registry: Export Control – Research
  https://www.archives.gov/cui/registry/category-detail/export-control-research.html


You’ve got this!!!

Special Thanks to:

Zena Hovda

Export Control Officer

San Diego State University and

San Diego State University Research Foundation

Andrea Deaton, CRA

Associate Vice President for Research and

Executive Director, Office of Research Services

University of Oklahoma

Questions? Contact me…

- Sandra Nordahl, CRA
  Director, Sponsored Research Contracting and Compliance
  and Facility Security Officer
  snordahl@sdsu.edu
  619.594.4172