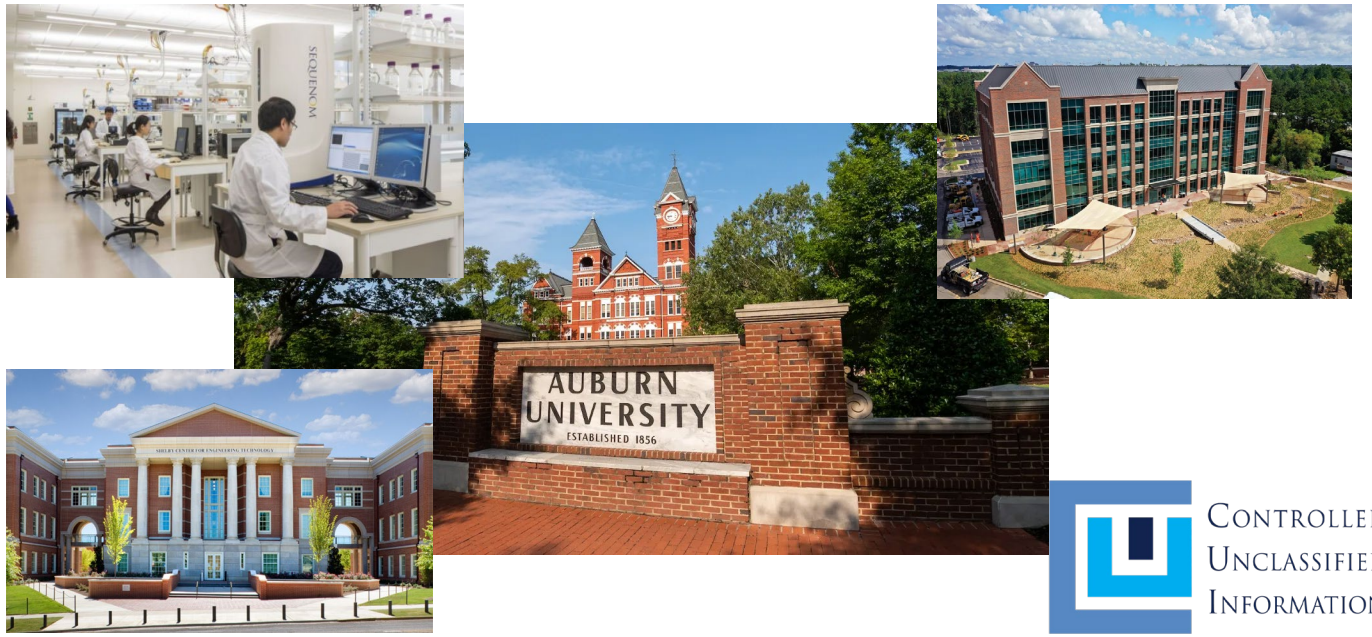
FOREIGN INFLUENCE AND THE FUTURE OF RESTRICTED RESEARCH



CONTROLLED
UNCLASSIFIED
INFORMATION

What is CUI?

- CUI stands for ***Controlled Unclassified Information***

- CUI is government created or owned information that requires safeguarding or dissemination controls consistent with applicable laws, regulations and government wide policies.
  - Executive Order 13556
  - 32 CFR Part 2002
  - NIST Publications

- CUI ***is not*** classified information. It is not corporate intellectual property unless created for or included in requirements related to a government contract.

- The National Archives and Records Administration (NARA) is the executive agent tasked with the implementation of CUI and has delegated these responsibilities to the Information Security Oversight Office (ISOO).

CONTROLLED
UNCLASSIFIED
INFORMATION

CUI Categories

- Ammonium Nitrate
- Chemical-terrorism Vulnerability Information
- Critical Energy Infrastructure Information
- Emergency Management
- General Critical Infrastructure Information
- Information Systems Vulnerability Information
- Physical Security
- Protected Critical Infrastructure Information
- SAFETY Act Information
- Toxic Substances
- ***Water Assessments***
- Controlled Technical Information
- DoD Critical Infrastructure Security Information
- Naval Nuclear Propulsion Information
- Unclassified Controlled Nuclear Information – Defense
- ***Export Controlled***
- ***Export Controlled Research***
- ***Agriculture***
- General Intelligence
- Geodetic Product Information
- Operations Security
- Budget
- Electronic Funds Transfer
- Federal Housing Finance Non-Public Information
- Financial Supervision Information
- General Financial Information
- Retirement
- ***Permanent Resident Status***
- Status Adjustment
- ***Visas***
- Accident Investigation
- DNA
- ***Contract Use***
- Death Records
- General Privacy
- Genetic Information
- Health Information
- Inspector General Protected
- Military Personnel Records
- Personnel Records
- ***Student Records***
- ***General Procurement and Acquisition***
- ***Small Business Research and Technology***
- Source Selection
- General Law Enforcement
- NATO Restricted
- NATO Unclassified
- General Nuclear
- ***Nuclear Security-Related Information***
- Safeguards Information
- Unclassified Controlled Nuclear Information – Energy
- ***Homeland Security Agreement Information***
- ***Homeland Security Enforcement Information***
- Information Systems Vulnerability Information - Homeland
- International Agreement Information - Homeland
- Operations Security Information
- Personnel Security Information
- Physical Security - Homeland
- Privacy Information
- ***Sensitive Personally Identifiable Information***

https://www.archives.gov/cui/registry/category-list

CONTROLLED UNCLASSIFIED INFORMATION

Why Is CUI Important?

- Foreign Influence
  - Federal agencies and policymakers have expressed concern that foreign entities may be using the academic research enterprise in an attempt to compromise the United States' economic competitiveness and national security.

- NIH Statement: "Unfortunately, threats to the integrity of U.S. biomedical research exist. NIH is aware that some foreign entities have mounted systematic programs to influence NIH researchers and peer reviewers and to take advantage of the long tradition of trust, fairness, and excellence of NIH supported research activities. This kind of inappropriate influence is not limited to biomedical research; it has been a significant issue for defense and energy research for some time."

- NSF Statement: "As partners in the scientific enterprise, U.S. universities and colleges must help promote scientific openness and integrity and safeguard information that impacts national security and economic competitiveness. The NSB recommends that all institutions conducting fundamental research supported by the National Science Foundation embrace transparency and rigorously adhere to conflict of interest and conflict of commitment policies. The Board also encourages those institutions to educate their communities about how to protect the integrity of research."

Controlled Unclassified Information

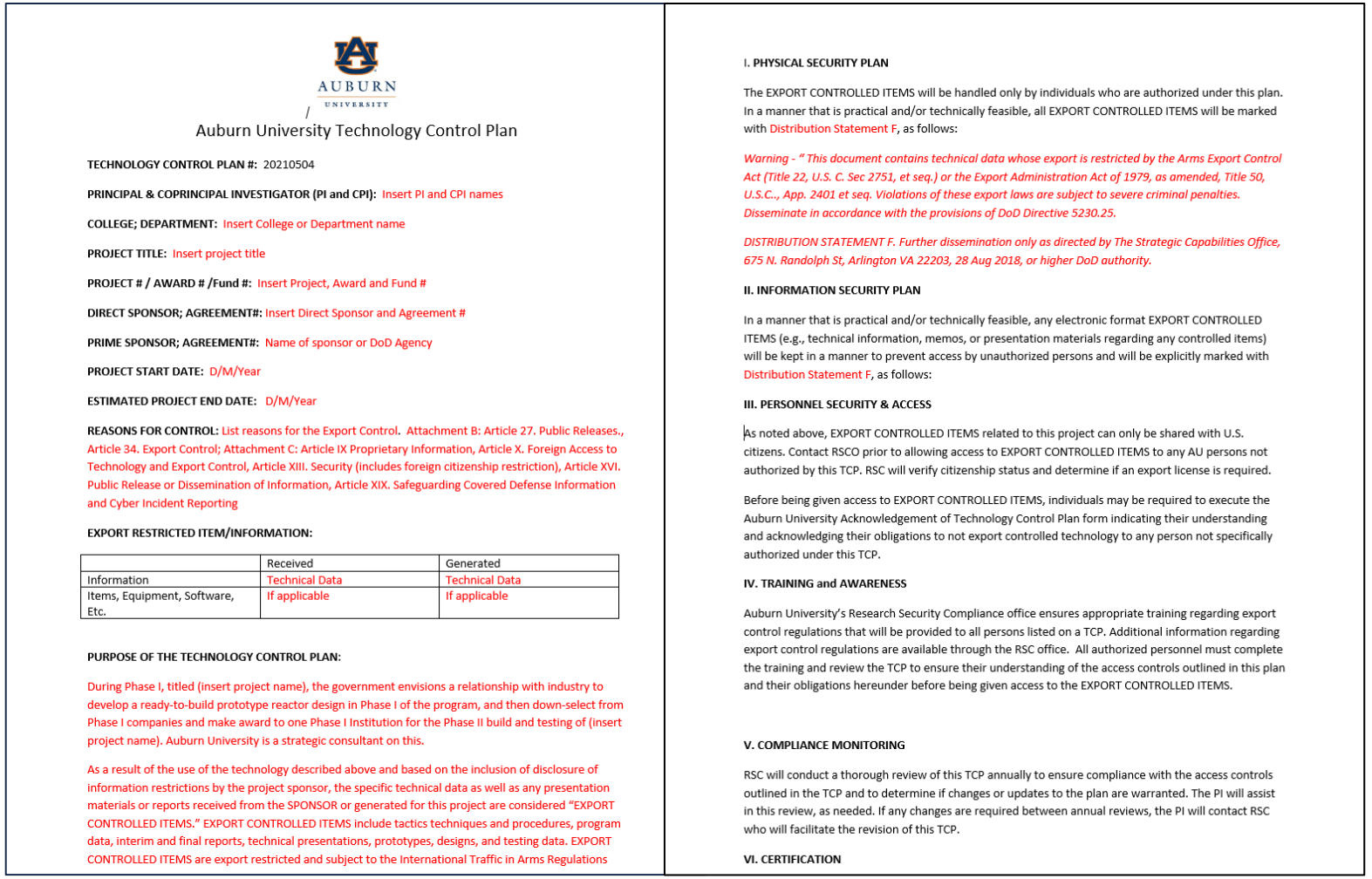
Foreign Influence Examples

- *"University Researcher Sentenced to Prison for Lying on Grant Applications to Develop Scientific Expertise for China"*
- *"Ph.D. Chemist Convicted of Conspiracy to Steal Trade Secrets, Economic Espionage, Theft of Trade Secrets and Wire Fraud"*
- *"Hospital Researcher Sentenced to Prison for Conspiring to Steal Trade Secrets and Sell to China"*
- *"Man Who Worked At Local Research Institute For 10 Years Pleads Guilty To Conspiring To Steal Trade Secrets, Sell Them In China"*
- *"NASA Researcher Arrested for False Statements and Wire Fraud in Relation to China's Talents Program: Texas A&M University Professor Working on U.S. Space Projects Allegedly Hid Affiliations with Chinese State Owned Academic and Commercial Institutions"*
- *"Researchers Charged with Visa Fraud After Lying About Their Work for China's People's Liberation Army"*
- Intellectual theft cost: $225 billion to $600 billion annually

CONTROLLED UNCLASSIFIED INFORMATION

What Does This Mean For You?

- Security is everyone's responsibility
- PI's agree to protect controlled information
- Technology Control Plan (TCP)
- Physical Security
  - Bldgs, locks, storage, safes, labs, equipment, barriers, etc
- Personnel Security
  - Who needs access?
  - Who can't have access?
- Cybersecurity
  - The Cybersecurity Maturity Model Certification (CMMC) is a unifying standard for the implementation of cybersecurity.
- Training



AUBURN UNIVERSITY

Auburn University Technology Control Plan

TECHNOLOGY CONTROL PLAN #: 20210504

PRINCIPAL & COPRINCIPAL INVESTIGATOR (PI and CPI): Insert PI and CPI names

COLLEGE; DEPARTMENT: Insert College or Department name

PROJECT TITLE: Insert project title

PROJECT # / AWARD # /Fund #: Insert Project, Award and Fund #

DIRECT SPONSOR; AGREEMENT#: Insert Direct Sponsor and Agreement #

PRIME SPONSOR; AGREEMENT#: Name of sponsor or DoD Agency

PROJECT START DATE: D/M/Year

ESTIMATED PROJECT END DATE: D/M/Year

REASONS FOR CONTROL: List reasons for the Export Control. Attachment B: Article 27. Public Releases., Article 34. Export Control; Attachment C: Article IX Proprietary Information, Article X. Foreign Access to Technology and Export Control, Article XIII. Security (includes foreign citizenship restriction), Article XVI. Public Release or Dissemination of Information, Article XIX. Safeguarding Covered Defense Information and Cyber Incident Reporting

EXPORT RESTRICTED ITEM/INFORMATION:

	Received	Generated
Information	Technical Data	Technical Data
Items, Equipment, Software, Etc.	If applicable	If applicable

PURPOSE OF THE TECHNOLOGY CONTROL PLAN:

During Phase I, titled (insert project name), the government envisions a relationship with industry to develop a ready-to-build prototype reactor design in Phase I of the program, and then down-select from Phase I companies and make award to one Phase I Institution for the Phase II build and testing of (insert project name). Auburn University is a strategic consultant on this.

As a result of the use of the technology described above and based on the inclusion of disclosure of information restrictions by the project sponsor, the specific technical data as well as any presentation materials or reports received from the SPONSOR or generated for this project are considered "EXPORT CONTROLLED ITEMS." EXPORT CONTROLLED ITEMS include tactics techniques and procedures, program data, interim and final reports, technical presentations, prototypes, designs, and testing data. EXPORT CONTROLLED ITEMS are export restricted and subject to the International Traffic in Arms Regulations

I. PHYSICAL SECURITY PLAN

The EXPORT CONTROLLED ITEMS will be handled only by individuals who are authorized under this plan. In a manner that is practical and/or technically feasible, all EXPORT CONTROLLED ITEMS will be marked with Distribution Statement F, as follows:

Warning - " This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S. C. Sec 2751, et seq.) or the Export Administration Act of 1979, as amended, Title 50, U.S.C., App. 2401 et seq. Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with the provisions of DoD Directive 5230.25.

DISTRIBUTION STATEMENT F. Further dissemination only as directed by The Strategic Capabilities Office, 675 N. Randolph St, Arlington VA 22203, 28 Aug 2018, or higher DoD authority.

II. INFORMATION SECURITY PLAN

In a manner that is practical and/or technically feasible, any electronic format EXPORT CONTROLLED ITEMS (e.g., technical information, memos, or presentation materials regarding any controlled items) will be kept in a manner to prevent access by unauthorized persons and will be explicitly marked with Distribution Statement F, as follows:

III. PERSONNEL SECURITY & ACCESS

As noted above, EXPORT CONTROLLED ITEMS related to this project can only be shared with U.S. citizens. Contact RSCO prior to allowing access to EXPORT CONTROLLED ITEMS to any AU persons not authorized by this TCP. RSC will verify citizenship status and determine if an export license is required.

Before being given access to EXPORT CONTROLLED ITEMS, individuals may be required to execute the Auburn University Acknowledgement of Technology Control Plan form indicating their understanding and acknowledging their obligations to not export controlled technology to any person not specifically authorized under this TCP.

IV. TRAINING and AWARENESS

Auburn University's Research Security Compliance office ensures appropriate training regarding export control regulations that will be provided to all persons listed on a TCP. Additional information regarding export control regulations are available through the RSC office. All authorized personnel must complete the training and review the TCP to ensure their understanding of the access controls outlined in this plan and their obligations hereunder before being given access to the EXPORT CONTROLLED ITEMS.

V. COMPLIANCE MONITORING

RSC will conduct a thorough review of this TCP annually to ensure compliance with the access controls outlined in the TCP and to determine if changes or updates to the plan are warranted. The PI will assist in this review, as needed. If any changes are required between annual reviews, the PI will contact RSC who will facilitate the revision of this TCP.

VI. CERTIFICATION

CONTROLLED UNCLASSIFIED INFORMATION

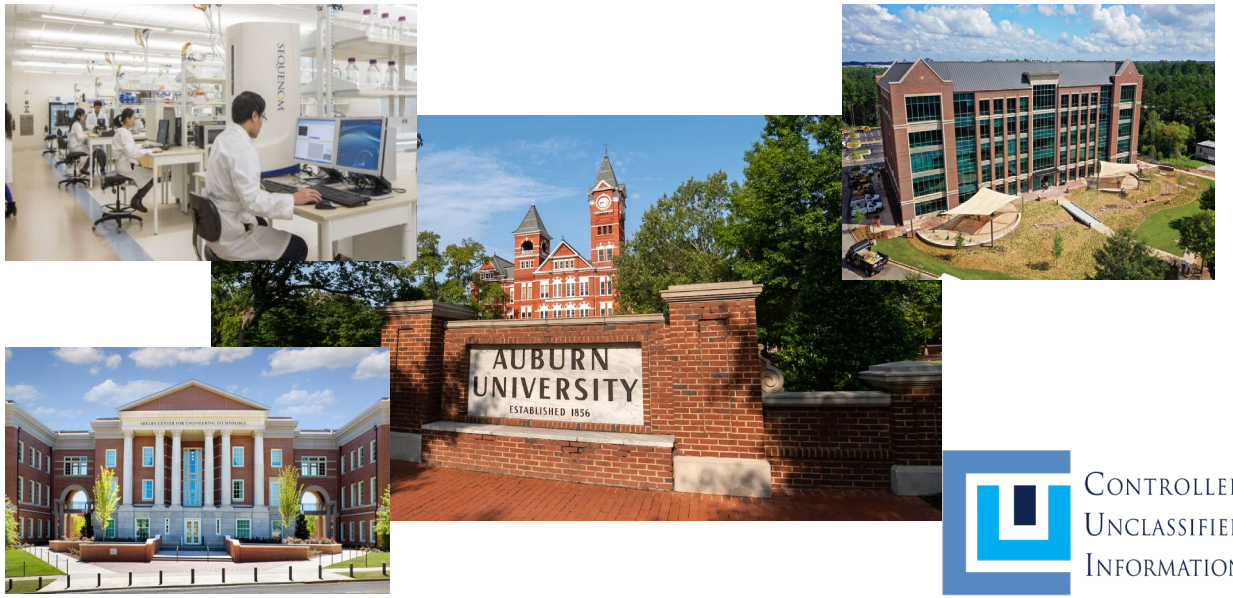
Contact Information

Tony A. Novara
Director, Research Security Compliance Office
Auburn University
2556 Woltosz Research Lab
Auburn, Al 36849
Office: (334) 844-5041
Tan0005@auburn.edu

Kevin J. Briggins
CUI Manager
Auburn University Office of Research & Economic Development
Research and Innovation Center
Auburn, AL 36849
Office: (334) 844-0266
Kjb0076@auburn.edu

Andrew L. Caldwell
Cybersecurity Manager
Auburn University Office of Research & Economic Development
Research and Innovation Center
Auburn, AL 36849
Office: (334) 844-0266
Alc0021@auburn.edu

QUESTIONS?



CONTROLLED
UNCLASSIFIED
INFORMATION