UNIVERSITY OF TEXAS ARLINGTON

Audit Report

Research - Controlled Unclassified Information

July 2022

OFFICE OF AUDIT AND CONSULTING SERVICES | BOX 19112 | ARLINGTON | TX 76019-0112 | 817-272-0150 | www.uta.edu/internalaudit

Summary – Research - Controlled Unclassified Information

We recently completed an audit of UTA's handling of Controlled Unclassified Information (CUI) for research grants. The background, audit objective, scope, and ratings are detailed on pages 6, 7, and 8 of this report.

Overall, the audit identified the need to improve research grant workflow, the quality of training records, and written documentation of controls. Specific observations from the audit are provided below:

Recommendations	Rating	Count
3	Priority	0
	High	0
	Medium	3
	Low	0

Observations	Recommendations	Rating	Page
A. Research Agreement Workflow	1. Consider formally memorializing the email and documentation protocol in place to solicit UTA Information Security Office (ISO) and Office of Information Technology (OIT) input on research agreements in cases where data security assertions are necessary.	Medium	Page 3
B. Training Records	2. Develop a training curriculum and materials related to the control and handling of Controlled Unclassified Information (CUI). Provide training classes and obtain written statements of understanding from the participants.	Medium	Page 4
C. Control Procedure Documentation	3. Document the general computing controls related to the Microsoft Government Community Cloud (GCC) High tenant.	Medium	Page 5

Further details can be found on the following pages. Other less significant opportunities were communicated to management separately.

We appreciate the outstanding courtesy and cooperation received from the Office of the Vice President for Research, Office of Research Administration, the Department of Mechanical and Aerospace Engineering, the Office of Information Technology, the Information Security Office, and the Division of Business Procurement and Payment Services.

Observation 1 – Research Agreement Workflow

Medium

The research agreement process is controlled by the Office of Research Administration. The federal government agency providing the agreement indicates that the project, either in full or part, is to be controlled as Controlled Unclassified Information (CUI). Research Administration has detailed written guidance and strategic protocols for negotiating agreements with federal officials to appropriately limit and identify CUI as being applicable. When required as a condition of the agreement, UTA provides written assurance to the federal agency stating that UTA's security controls are adequate to protect project documentation to the finally agreed upon standards. The UTA Information Security Office (ISO), Office of Information Technology (OIT), and project Principal Investigator, as applicable, are routinely consulted by the Agreement Manager as to the security/data standards to be agreed upon by the university, but not formally included in a written agreement workflow and not consistently copied on the written assurances finally provided to the federal agency. Adopting an internal written protocol to formally document the current solicitation of the ISO/OIT input on research agreements may be of benefit to UTA in cases where data security assertions are necessary.

Recommendation:

Consider formally memorializing the email and documentation protocol in place to solicit UTA Information Security Office (ISO) and Office of Information Technology (OIT) input on research agreements in cases where data security assertions are necessary.

Management Response:

The Agreement Manager will share copies of agreements with the ISO and OIT that will or expect to receive CUI or controlled information. Research Administration will create a written Standard Operating Procedure (SOP) to document the process. In addition, the ISO, OIT and Research Administration have a workgroup formed to codify the service offering for researchers to secure their research data, including compliant CUI systems and tools. These resources along with the compliance requirements of individual agreements will be references for the SOP to be created.

Target Implementation Date:

September 1, 2022

Responsible Party:

Assistant Vice President for Research Administration

Observation 2 – Training Records

Medium

The National Institute for Standards and Technology (NIST) Special Publication 800-171r2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, requires the retention of training records. Written evidence of training related to Controlled Unclassified Information (CUI) does not exist.

Eight researchers are engaged on the two projects in the CUI pilot program. Both projects are under the control of researchers from the UTA Department of Mechanical and Aerospace Engineering.

One of the research teams created a CUI policy document that is used to provide training to the researchers on the project. However, training records are not retained by the team lead. The other team has not received formal training.

We interviewed 5 of the 8 researchers engaged on these projects and conducted a walkthrough of one research facility. We determined that the team members are fully aware of the CUI marking standards and general safe handling of CUI.

Recommendation:

Develop a training curriculum and materials related to the control and handling of Controlled Unclassified Information (CUI). Provide training classes and obtain written statements of understanding from the participants.

Management Response:

Research Security training, including CUI specific content, is already part of the Draft Research Security Plan for National Security Presidential Memorandum – 33 (NSPM-33). We are exploring curriculum content in the Collaborative Institutional Training Initiative (CITI Program) and the National Science Foundation (NSF) has stated they intend to develop research security training as part of their responsibilities under NSPM-33. We will continue to explore these developments along with coordinating OIT and ISO employee annual training requirements related to cybersecurity. As part of the CUI process, the System Security Plan itself is a training document specific to the security of that project specific CUI. These materials will be reviewed and incorporated into a formal CUI training module as required training for anyone authorized to access CUI.

Target Implementation Date:

December 1, 2022

Responsible Party:

Assistant Vice President for Research Administration

Observation 3 – Control Procedure Documentation

Medium

The National Institute for Standards and Technology (NIST) Special Publication 800-171r2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, requires written control procedures. The Office of Information Technology has not written general computing control procedures for the Microsoft 365 Government Community Cloud (GCC) High tenant. This tenant was established approximately two months prior to the start of the audit specifically for one of the Controlled Unclassified Information (CUI) pilot projects.

Recommendation:

Document the general computing controls related to the Microsoft Government Community Cloud (GCC) High tenant.

Management Response:

The Information Security Office will assist in developing or strengthening security policies for Research based on NIST SP 800-171r2 for the protection of controlled unclassified data. OIT, in cooperation with the Office of the Vice President for Research, will develop general computing control procedures to enforce security policies developed to harden the Microsoft 365 GCC High tenant.

Target Implementation Date:

May 1, 2023

Responsible Party:

Chief Information Officer, Office of Information Technology

Background – Research - Controlled Unclassified Information

Background

Executive Order 13556 established a Controlled Unclassified Information (CUI) Program to standardize the way the executive branch handles unclassified information that requires protection. Only information that requires safeguarding or dissemination controls pursuant to federal law, regulation, or governmentwide policy may be designated as CUI. The CUI Program is designed to address several deficiencies in managing and protecting unclassified information to include inconsistent markings, inadequate safeguarding, and needless restrictions, both by standardizing procedures and by providing common definitions through a CUI Registry.

UTA's primary computing environment is not designed to safely store and handle Controlled Unclassified Information or otherwise classified information. As a result, UTA researchers are unable to attract and secure projects of this nature. Research Administration, working in conjunction with the Office of Information Technology, has created secure enclaves to support two research projects required to be controlled as CUI. One enclave is a cloud-based solution, and the other is located on the UTA main campus. Research Administration, taking a risk-based approach to the implementation process, is utilizing these two projects as a pilot program to develop standardized controls and procedures based on the National Institute for Standards and Technology (NIST) Special Publication 800-171r2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*.

Defense Federal Acquisition Regulations Supplement (DFARS) 252.204-7112 requires contractors to perform NIST 800-171 assessments regularly (252.204-7019) and to maintain a Cybersecurity Maturity Model Certification (CMMC) (252.204-7021). UTA is required to obtain the appropriate CMMC certification by 2025.

Audit Objective, Audit Scope and Methodology – Research - Controlled Unclassified Information

Audit Objective

The objective of the audit was to determine whether research-related Controlled Unclassified Information (CUI) is being managed in accordance with best practices and guidance.

Additional objectives of the audit were to determine whether:

- The CUI Program is designed to effectively identify research information that should be controlled as CUI.
- Access controls are designed to effectively restrict access to CUI to those with a lawful government purpose.
- Users are properly trained to handle CUI.
- Documents and media are marked appropriately and adequately protected.

Audit Scope and Methodology

As part of this audit, we evaluated four primary aspects of the CUI program:

1. Detection of research projects that should be controlled as CUI,
2. Access controls related to the two research projects in the CUI pilot program,
3. Training of users in the control and handling of CUI, and
4. Marking and protection of documents and other electronic media.

Our examination was conducted in accordance with the Institute of Internal Auditor's *International Standard's for the Professional Practice of Internal Auditing.*

Ranking Criteria – Research - Controlled Unclassified Information

Ranking Criteria

All findings in this report are ranked based on an assessment of applicable qualitative, operational control and quantitative risk factors, as well as the probability of a negative outcome occurring if the risk is not adequately mitigated. The criteria for these rankings are as follows:

Priority	An issue identified by an internal audit that, if not addressed on a timely basis, could directly impact achievement of a strategic or important operational objective of UTA or the UT System as a whole.
High	A finding identified by an internal audit that is considered to have a medium to high probability of adverse effects to UTA either as a whole or to a significant college/school/unit level.
Medium	A finding identified by an internal audit that is considered to have a low to medium probability of adverse effects to UTA either as a whole or to a college/school/unit level.
Low	A finding identified by an internal audit that is considered to have minimal probability of adverse effects to UTA either as a whole or to a college/school/unit level.

None of the findings from this review are deemed as a “Priority” finding.

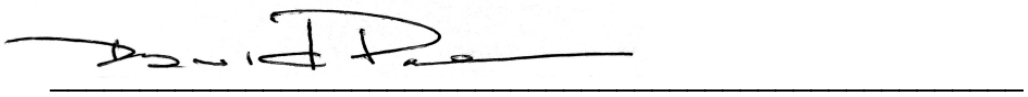
Distribution – Research - Controlled Unclassified Information

To:	Jennifer Cowley	*President, UTA*
	Randal Rose	*Audit Committee Chairman*

Audit Committee:

Pranesh Aswath	*Interim Provost and Vice President for Academic Affairs, UTA*
Shelby Boseman	*University Attorney and Chief Legal Officer, UTA*
John Davidson	*Associate Vice President and Interim Chief Financial Officer, UTA*
Helen Dickey	*Partner, Harris & Dickey LLP*
Harry Dombroski	*Dean, College of Business, UTA*
Jacqueline Fay	*FY 2022 Faculty Senate Chair (Associate Professor, English), UTA*
John Hall	*Vice President for Administration and Campus Operations, UTA*
Chris Mitchell	*Chief Diversity Officer, Crowe LLP*
Bryan Samuel	*Vice President for Diversity, Equity and Inclusion, UTA*
Jewel Washington	*Chief Human Resources Officer, UTA*

From: David Price — *Chief Audit Executive, UTA*



cc:	Jennifer Chapman	*Compliance Officer, UTA*
	Jeremy Forsberg	*Assistant Vice President, Research Administration, UTA*
	James Grover	*Dean of the Graduate School and Interim Vice President for Research, UTA*
	Jeffery Neyland	*Chief Information Officer, Office of Information Technology, UTA*
	Cheryl Nifong	*Chief Information Security Officer, Information Security Office, UTA*

Auditor in Charge:

Greg Baviera	*Senior IT Auditor II, UTA*