

Export Control & Research Cybersecurity Office

Ask RCRA June 12, 2025



EMORY
UNIVERSITY

Research Compliance and Regulatory Affairs
Research Administration



Export Control
and Research
Cybersecurity
Office
(ECRC)

Why Export Control and Research Cybersecurity?

- Research related cybersecurity regulatory requirements.
 - **DoD's DFARS 252.204-7012 clause**
 - Adequate Security, Cyber Incident Reporting; Flow down Requirements; NIST SP 800-171 Compliance
 - **Cybersecurity Maturity Model Certification (CMMC)**
 - Standardized framework developed by the DoD to protect sensitive unclassified information
 - Baseline requirements for storing, transmitting, accessing, or working with Federal Contract Information (FCI) or Controlled Unclassified Information (CUI).
 - **NIH Genomic Data Sharing Policy**
 - Institutional systems used to access or store covered data must be compliant with NIST SP 800-171
 - **New FAR Rule implementing the Controlled Unclassified Information (CUI) program**
 - We will likely see increased CUI designation in the near future
 - NIST 800-171 compliant systems

Next Steps

- Develop programmatic components for new responsibilities related to Research Cybersecurity
 - Written Policies and Procedures
 - Compliance Oversight
 - Training and Education
 - Internal Monitoring
- Office Rebranding and Updated website to include information on CUI and research cybersecurity resources



Export Control
and Research
Cybersecurity
Office
(ECRC)

ECRC Team



Rose Ndegwa
Director



Shelby Still
Assistant Director

Questions? Please reach out to us!

Email : exportcontrol@emory.edu

Phone:

404-251-5185

404-896-7570