**Technology Control Plan Process**

**“Technology Control Plans”** (TCP) are primarily implemented when a project involves “**Controlled Unclassified Information”** (CUI) or when required by the grant award. The TCP ensures adherence to U.S. Export Control laws and regulations as well as to “**International Traffic in Arms Regulations”** (ITAR) Compliance Policy and Procedures. TCPs further outline how sensitive information will be protected, including making sure proper security measures are in place and ensuring that only authorized individuals have access to the CUI. For those investigators for whom a TCP is required or otherwise necessary the following steps will occur:

1. An assessment will be completed by the Director of Information Security, IT Services, with input from other university personnel, to determine what technology and network infrastructure needs to be incorporated within the TCP.
2. A customized TCP will be developed and signed by the Principal Investigator (PI) and the Executive Director of ORSP. Annually, the TCP will be reviewed by the PI and the Executive Director and re-signed.
3. Prior to commencing work, the PI and other personnel on the research project who have direct access to the controlled information will be required to take the CITI training program on Export Controls. Every three years thereafter, the refresher course will be required.
   1. Citi Export control training course: https://about.citiprogram.org/course/export-compliance-ec/
   2. Citi Export control refresher course: https://about.citiprogram.org/course/ec-refresher/
4. For all projects, record retention requirements must be specified in the TCP and implemented.
5. All PIs and personnel who fail to comply with the applicable TCP will be subject to discipline, up to and including termination.