**TITLE**: Technology Control Plan Assessment Procedure

**PURPOSE:** Maintaining CU Boulder’s Export Compliance Program by conducting annual on-site assessments of Technology Control Plans (TCP) in order to verify that the controls put in place by the TCP are in accordance with the TCP on file. In addition, procedures and records designed to ensure adherence with export control laws and regulations may also be reviewed. Internal assessments are integral to the University’s and researchers’ interests in detecting, correcting, and preventing potential violations before external audits are conducted.

**RESPONSIBILITY:** The ORI QA/QI Office Staff will be responsible for the execution of the SOP.

 **APPROVAL:** The Associate Vice Chancellor of Research Integrity & Compliance (Joe Rosse) approved this SOP as of 1/14/2019.

**PROCEDURES:**

1. TCP Selection
	1. At the beginning of every month, select 1 TCP to be assessed from the list of active TCPs. For the time being, only 1 TCP will be assessed per month and each TCP will be assessed annually.
2. PI Contact and Activities Prior to Assessment:
	1. Submit a security review request for the selected TCP to itso-sec-review@colorado.edu.
	2. Include the following information in the email request:
		1. Type (TCP Yearly Audit)
		2. Attach a PDF of the TCP
		3. List Main Contacts/PI(s) on TCP
		4. Propose dates (within the next 4 weeks) for an on-site visit (based on the Research Cybersecurity Program Manager and the ORI QA Specialist’s availability)
	3. Contact the principal investigator (either by phone or email) to notify them that their TCP has been selected for an onsite review, CC-ing the OEC. The following may be included in and requested:
		1. The purpose of the assessment and a summary of items that will be discussed/reviewed during the visit.
		2. How the protocol was selected and the annual nature of the assessment.
		3. Confidentiality of the review
			1. No information gathered from the review will be shared with anyone other than the project’s personnel, the Research Cybersecurity Program Manager, the QA/QI Office and the OEC.
		4. Given The Research Cybersecurity Program Manager availability, propose dates (before the end of the month) for an on-site visit and request that the contact chooses one.
	4. Review the TCP for compliance to OEC procedures and tailor assessment worksheet with the selected TCP’s information and IT cybersecurity information gathered from the security review request.
3. During the On-Site Assessment:
	1. The Research Cybersecurity Program Manager will join the ORI QA Specialist for the IT Cybersecurity portion of the on-site assessment visit.
	2. Conduct an opening meeting discussing the following:
		1. Purpose, benefits, and scope of assessment.
		2. A tentative schedule for the on-site assessment
		3. The process that occurs if any non-compliance is discovered during the onsite visit.
		4. Q/A
	3. Perform an audit of the TCP, utilizing the TCP assessment worksheet to interview the PI, check any relevant records, and observe control measures put in place.
		1. Corroborate the IT Cybersecurity information gathered from the on-site assessment and security measures outlined on the TCP with the IT cybersecurity information from the security review request.
	4. Any findings that arise that may indicate a violation or a need to amend a TCP. In this circumstance, findings will not be immediately discussed with the PI or lab. Findings will be brought to the OEC for discussion in a timely manner, in the form of a preliminary report rough draft. Any action to be taken based on observational findings from the assessment will be decided by the OEC staff.
		1. Finalize the preliminary report based on feedback given from the OEC and prepare it for delivery to the assessed PI and laboratory.
4. After the On-Site Assessment:
	1. With the Research Cybersecurity Program Manager, conduct a Preliminary Report Delivery Meeting with the PI and laboratory. Discuss the following:
		1. Findings discovered during the onsite assessment.
		2. The corrective action process required for those findings (See the Corrective Action Process Procedure).
		3. If the PI presents significant evidence during the meeting that a finding(s) on the preliminary report is not legitimate, the finding may be taken off the preliminary report. In this instance, the OEC will be notified.
	2. If no evidence of noncompliance or disclosures to a foreign national are found during the onsite assessment, a meeting is not necessary and will not be held, and the report will be emailed to the PI, reflecting that no issues were observed and no further action is required.
		1. If the PI requests to have a meeting regardless of the flawless assessment report, a meeting will be scheduled to take place to accommodate the PI.
	3. Deadlines for corrective action to take place will vary based on report findings, and will be decided with consultation from the OEC and presented during the preliminary report delivery meeting.
		1. It is the Research Cybersecurity Program Manager’s responsibility to hold the PI accountable for resolving any required TCP correction action related to cybersecurity. He will relay it’s completion to the QA/QI Office so it can be documented in the final report.
		2. It is the QA/QI Office’s responsibility to hold the PI accountable for resolving any required TCP correction action in accordance with the set deadlines (See the Corrective Action Process Procedure).
		3. If the deadline to correct any noncompliance is not met, that can be grounds for terminating a TCP, at the Associate Vice Chancellor of Research’s discretion.
	4. Once the findings have been resolved through corrective action, a Final Report will be issued to the assessed PI and OEC and the assessment will be considered ‘closed-out.’ No further action is necessary beyond this point.