IMPLEMENTATION & MANAGEMENT GUIDANCE FOR FACULTY

NU-RES RESEARCH COMPLIANCE
RESEARCHCOMPLIANCE@NORTHEASTERN.EDU
617-373-5600

Table of Contents

Introduction to Export Controls, Controlled Unclassified Information (CUI) & This Guide

Export Controls
The United States Federal Government utilizes Export Controls to protect the U.S. economic and security interests. Export Control regulations extend to both the parties that U.S. businesses and entities engage with, as well as materials, data and access to controlled materials and data. Export Control Regulations are regulated and overseen by the following agencies:

Dept. & Regulatory Agency	Regulations	Items Controlled
Department of Treasury *Office of Foreign Assets Controls (OFAC)*	Foreign Assets Control Regulations (FACR)	⇒ Travel abroad ⇒ Transactions with foreign individuals & entities ⇒ Transactions with specific foreign countries (i.e., Iran) ⇒ Export and import of items
Department of Commerce *Bureau of Industry and Security (BIS)*	Export Administration Regulations (EAR) via the Commerce Control List (CCL)	⇒ Dual-use goods, software & technology used predominantly in civilian settings, but that may have military applications ⇒ EAR99 items will civilian application only ⇒ Anti-boycott provisions
Department of State *Directorate of Defense Trade Controls (DDTC)*	International Traffic in Arms Regulations (ITAR) via the U.S. Munitions List (USML)	⇒ Defense articles & technical data ⇒ Goods, software, or information specifically designed, developed, or modified for military or intelligence application ⇒ Defense services
Department of Energy *Nuclear Regulatory Commission (NRC)*	Export and Import of Nuclear Equipment and Material Regulations (EINEMR) & Assistance to Foreign Atomic Energy Activities Regulations (AFAEAR)	⇒ Nuclear equipment, materials, software, and technology

As an academic institution, Northeastern primarily performs fundamental research, meaning that the results are intended to be shared with the broad, global scientific community through a variety of mediums, including publications, conferences, etc., and there are no restrictions on the access to and dissemination of the research results from the sponsor.

However, Northeastern, including and especially its subsidiary, KRI, LLC, do undertake some research and development activities for the government which may contain information controlled under either the EAR or ITAR regulations. In such cases, Northeastern must protect the research activities in accordance with the expectations set forth by the relevant funding agencies. The primary mode of doing this is to work with the faculty member(s) engaged in the project to generate a Technology Control Plan (TCP).

Controlled Unclassified Information (CUI)

Controlled Unclassified Information (CUI) is defined by 32 CFR 2002.1(h) as

> *[I]nformation the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.*

Sample CUI Categories for reference **Full list of subcategories can be found in CUI Category List Archives**	
Critical Infrastructure	North Atlantic Treaty Organization (NATO) o NATO Restricted o NATO Unclassified
Defense or Covered Defense Information (CDI): o Controlled Technical Information o DoD Critical Infrastructure Security Information o Naval Nuclear Propulsion Information o Unclassified Controlled Nuclear Information-Defense	Nuclear: o General Nuclear o Nuclear Recommendation Material o Nuclear Security-Related Information o Safeguards Information o Unclassified Controlled Nuclear Information - Energy
Export Control: o Export Controlled (EAR dual-use and ITAR) o Export Controlled Research	Patent: o Patent Application o Inventions o Secrecy orders
Finance	Privacy
Immigration	Procurement and Acquisition
Intelligence	Proprietary Business Information
International Agreements	Provisional
Law Enforcement	Statistical
Legal	Tax
Natural and Cultural Resources	Transportation

A common set of safeguarding controls for some categories of CUI are contained in NIST Special Publication (SP) 800-171. However, each category of CUI must be consulted separately to determine the applicable safeguarding and / or dissemination controls.

It is important to note that there may be some instances where information is CUI but is not export-controlled (e.g., privacy information, tax information). Conversely, all CDI and export-controlled projects are CUI categories. Reference table above.

CUI must be protected pursuant to all contracts and Other Transaction Authorities (OTAs) that include:

- ⇒ FAR 52.204-21 Basic Safeguarding of Covered Contractor Information Systems;
  - Contracts that only have this clause will not need a TCP
- ⇒ DFARS 252.204-7012 Safeguarding Covered Defense Information (CDI) and Cyber Incident Reporting;
- ⇒ DoD Instruction 8582.01 Security of Unclassified DoD Information on Non-DoD Systems;
- ⇒ Reference to Distribution Statements other than Distribution A;
- ⇒ Requirements to safeguard in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, NIST SP 800-171; and/or
- ⇒ Other proper prohibitions on the release and dissemination of data and/or access by non-U.S. Persons.

If contracts or OTAs are issued by a Department of Defense (DoD) agency that generate or receive CUI, the project will require adherence to all the policies and procedures set forth by the university related to the applicable protections.

Some CUI projects may utilize different environments or controls. The TCP is critical to help faculty and administration understand which controls are applicable and should be implemented at the applicable project stages.

This Guide

This guide is intended to provide faculty that are or will be working on a project where a TCP will be utilized with resources, especially guidance on the use and management of the TCP. This guide is not intended to be an exhaustive review of CUI, but rather to focus on recognizing the need for, the implementation of and the management of a TCP.

	Export Controls	**CUI**
Is it Fundamental Research?	No	It depends
Publication of results	Requires prior approval	Depending on category, may require approval
Labelling	Required by CUI rules	Depends on the CUI, but it is a best practice
Access by non-U.S. Persons	May require a license prior to granting access	It depends on the category
Security Protocols	As outlined in the TCP	As outlined in the TCP and required by CUI Policies

Export Controls throughout Northeastern

Northeastern, including all its global campuses and subsidiaries, including KRI, LLC, comply with these regulations in accordance with this TCP Guidance, the NU-RES Export Control website, the Export Control Manual and the Northeastern Policy on Export Control.

NU-RES Research Compliance is responsible for organizing and implementing the research-related export program through its Export Control and Logistics Analyst (ECLA) or the Research Security Officer, in coordination with the Director for Research Integrity & Export Controls. Please connect with us by reaching out to researchcompliance@northeastern.edu

Defining the Purpose and Scope of a TCP

A TCP must be utilized when the project will or may generate or receive export-controlled information or certain categories of CUI (e.g., CDI). The goal of the TCP is to prevent access by unauthorized individuals to export-controlled information or CUI. CUI data may not always require a TCP, the type of CUI should be analyzed by Research Compliance and a determination made about the appropriate controls, if applicable.

A TCP is prepared by Research Compliance in collaboration with the Principal Investigator and any other lead personnel or gatekeeper. Typically, TCPs are project-specific, but there may be two or more closely related projects that could be incorporated under a single TCP.

TCPs may include requirements such as physical security, information security, personnel responsibilities, and sponsor/contractual obligations. A TCP sets forth the expectations and procedures for protecting the research activities and resulting data, including defining who will be granted access to the activities, materials, and data. A TCP can also be utilized to outline which research activities are fundamental research, or EAR 99 and therefore not subject to the controls of the TCP (such activities may include participation by non-U.S. persons).

Unless otherwise specified, physical and information security requirements are based on a "one lock" principle, that is, there must be at least one lock between a controlled item and an unauthorized party to prevent access by that unauthorized party.

A TCP template is maintained by Research Compliance with TCP security guidance outlined in this document. TCPs must be approved by the PI and Research Compliance. Once a TCP is in place, the PI must routinely review the TCP and report any changes in personnel, security and/or scope of the work. Additionally, the Research Compliance will coordinate an annual review of the TCP with the PI/Responsible person or, to ensure continued compliance, as well as accurate dates, details and approved staff and students assigned to the project. All parties working on a controlled project must read the TCP and sign an acknowledgement of the restrictions prior to authorization for access to restricted research materials.

Finally, it is worth stating that the final TCP may be more or less restrictive than the controls described in this Guide. The controls will be based on several factors, including the type of research, contract requirements and the jurisdiction analysis performed by Research Compliance. This Guide is intended to provide some guidance around common costs, controls and questions that arise during the conduct of controlled research activities.

When TCPs are Utilized

The need for a TCP is often identified at the proposal stage when the funding agency or non-federal sponsor indicates if they believe some types of CUI such as CDI and export-controlled information will be shared or generated during the project. Northeastern may make a case that its proposal is for fundamental research, but if the funding opportunity includes an expectation that some or all the work will be controlled, it is likely the final contract will contain provisions that obligate the university to implement controls. In such cases, a TCP must be utilized to protect export-controlled information or CDI. TCPs may also be utilized when a project includes security controls or other access controls, such as sponsor prior approval requirements for all or any non-U.S. person participation.

If portions of the research are identified as fundamental or EAR 99, they will be described in the TCP.

Key Offices & Roles

Office of Information Security (OIS) & Information Technology Services (ITS)
The Office of Information Security (OIS) helps Northeastern to secure critical university resources ranging from student data to research data. OIS is a part of the ITS team and is focused specifically on ensuring data stewardship adheres to university and funding agency expectations. OIS can provide support at many stages, including consulting with faculty on potential solutions to manage large data sets, as well as training. ITS will set up GCC accounts for authorized personnel, provide training specific to the GCC account use. These accounts are controlled and monitored by ITS.

Research Compliance
Research Compliance is a part of Northeastern University Research Enterprise Services (NU-RES). NU-RES is responsible for helping to identify, mitigate, and manage a range of compliance issues for the University, including research integrity, export controls, controlled unclassified information (CUI), training, and policy management for research activities throughout Northeastern.

Research Compliance will generate TCPs or other access control plans for other export-controlled items, technology, and CDI/CUI.

Research Computing
Research Computing is responsible for providing high-performance computing solutions throughout the university. Research Computing is a critical part of Northeastern's data management and stewardship strategy. They can work with you on many aspects of your project, from technical writing to access to secure computing clusters.

KRI Facility Security Office
Northeastern, through its wholly-owned subsidiary, KRI, LLC (KRI, LLC) has a Facility Clearance managed by its Facility Security Office (FSO), which has the necessary policies, procedures, equipment, and space to safeguard classified information, items, and technology.

Classified work may only be executed in specific suites and spaces at the KRI Burlington campus. No other Northeastern campus, facility or space is currently cleared to receive classified information or perform classified work.

Classified Research

The United States government controls national security information by classification. These standards are laid out in the National Industrial Security Program Operating Manual (NISPOM), applicable Industrial Security Letters (ISLs) and Intelligence Community Directives (ICDs).

Classified materials at KRI, LLC are safeguarded in accordance with the NISPOM, and applicable ISLs and ICDs. Safeguarding classified materials is also in compliance with guidance from DSS and IC security personnel, which is incorporated in the KRI, LLC's Security Practices and Procedures (SPPs), and facility specific SPPs.

When a project contains both classified and export-controlled information, Research Compliance and the KRI, LLC FSO work together with the PI and project team to meet the obligations set forth by the relevant standards and regulations.

U.S. Persons & Deemed Exports

A deemed export is the release of controlled technology to a foreign person in the U.S., the knowledge of process, methods, and specifications, gained in the course of the project may be retained by that individual and has been "deemed" to be exported to the foreign person's country or countries of nationality (EAR Part 734 (b)). The knowledge and expertise they bring home with them is equivalent to putting that information on a flash drive and shipping it to the country in question. Therefore, it is important for Research Compliance to understand and analyze the proposed project team composition, even if nothing is being physically shipped outside of the U.S.

U.S. Persons are defined by EAR Part 772 and ITAR 120.15 as:
- ⇒ Any individual who is a U.S. citizen;
- ⇒ Any individual who is granted U.S. permanent residence (Green Card holder);
- ⇒ Any individual who is granted status as a "protected person" under 8 U.S.C. 1324b(a)(3), specifically refugees and asylees;
- ⇒ Any corporation/business/organization incorporated under U.S. law; or
- ⇒ Any part of the U.S. government.

Non-U.S. Persons include:
- ⇒ Any individual who is here on a visa (such as an F-1, H-1B, or J-1);

⇒ Any foreign corporation/business/organization not incorporated or organized under U.S. law; or

⇒ Foreign government and any agency or subdivision of foreign governments (e.g. diplomatic missions).

Difference Between a TCP & DD254

Department of Defense Form 254 (DD 254) is "Contract Security Classification Specification" [which] provides a contractor (or a subcontractor) the security requirements, classification guidance and handling procedures for classified material received and/or generated on a classified contract."[1]

TCPs are utilized to protect CUI, while DD 254's are used to identify and outline the protection of classified information. A project may have both a DD254 and a TCP. In such cases, it is common that the TCP would cover the entire project while the DD254 might cover specific, classified components of the project.

Work under a TCP will be conducted in specified lab space, but could be conducted at Northeastern, while work under a DD254 must take place at KRI, LLC.

Project aims that involve a DD254 will require additional protection and guidance. At Northeastern, the only component of the University equipped to protect classified information is KRI, LLC. Please work with the KRI Facility Security Office to review and establish appropriate procedures for DD254 (classified) work.

Common TCP Controls

List of Personnel: U.S. Persons or Deemed Export Licenses

All personnel working on the TCP must be identified in the TCP documentation. The list of personnel must be updated routinely, as the project team changes.

List of Personnel: Identifying Data Stewardship Roles

All personnel working on the TCP must also identify their role in CUI data management. All roles are described in the TCP. If you have any questions about what the roles and responsibilities entail, please reach out to Research Compliance.

Government Cloud Computing (GCC) & Secure Computing Clusters

Each project and associated sponsorship agreement will be analyzed to determine and implement the applicable security and dissemination controls specific to that project. Generally, Northeastern ITS has a secure computing instance called Government Cloud Computing (GCC), which includes access to email and video conferencing solutions.

Most projects will manage controlled project computing through GCC. This cloud-based, government-approved instance for secure computing should be used to store CUI, including export-controlled information. Under a project-specific TCP, CUI may only be stored on the ITS-

[1] https://acqnotes.com/acqnote/tasks/dd-form-254#:~:text=DD%20Form%20254-,DD%20Form%20254,generated%20on%20a%20classified%20contract.

approved instance or a department-maintained server, if the latter meets the information security requirements designated in the applicable contract. Classified information is neither stored nor processed on these servers. To request a GCC account, you must have a project that contains CDI, CUI and/or export-controlled information. Accounts should be requested for each individual on the TCP that will be interacting with the covered data.

For projects that are more data intensive, the university's Research Computing group has secure computing clusters, or individual labs may also elect to stand up a secure computing cluster. If you will be working with large amounts of data, it may be prudent to schedule a consultation with Research Computing and/or the Office of Information Security (OIS) to discuss the best solution for your project at the proposal stage. The costs associated with using or standing up a cluster should be included in your proposal. They are allowable direct costs.

Securing Lab Space or Remote Computing Space

All restricted activities require ensuring the space is secure before and during the activity and that all controlled materials and data are secured after the activity.

In Northeastern space, this could involve ensuring no one is able to see into the lab during work time and locking the space from entry during work time on a restricted project. Upon completion of the work, the materials, data, and information should be secured in something like a secure lockbox, cabinet, or secure container that only approved personnel have access to. This can be complex in some spaces, see the planning considerations section on lab space for more detail.

Meeting rooms may need similar protections (such as closing blinds and erasing boards before exiting the room). In addition, the project team may need to be sensitive to where they discuss the project, including not discussing it in elevators or open plan work areas.

It is important to note that if personnel will be accessing data or information remotely that they follow these same principles. As an example, if someone on the project team lives with a person who is not authorized to access the information, the project personnel would need to ensure that the individual is not able to see their computer screen at home or hear discussion of the project on a call (i.e., not sitting together in a room working).

Expectations for how restricted research should be executed for security purposes prior to, during, and after the research activities will be described in your TCP. It is incumbent upon the PI to ensure they are able to secure the space according to the TCP and that all students are trained in the importance and logistics of security.

Electronic Mail

Per the University's Policy on the Appropriate Use of Computer and Network Resources, all users may only use a university account to conduct university business and "unauthorized use of information systems/services is prohibited". Any electronic correspondence related to restricted research must be done using an approved Northeastern GCC account.

Training Requirement

All personnel working on restricted research or having access to CDI, export control CUI or defense articles or services must take the trainings required by University policy and/or those required by the TCP certification. Personnel participating in such research projects must retake the applicable trainings every three (3) years or as required by university policy.

In accordance with the NISPOM, ISL 2016-02, and the DSS Process Manual for the Certification and Accreditation of Classified Systems under the NISPOM Change 2 Version 3.3 (May 2016), KRI, LLC has implemented an Insider Threat Program. This program is established to deter, detect, and mitigate insider threats. The Facility Security Officer serves as the Insider Threat Program Senior Officer (ITPSO). Personnel working at KRI may be required to participate in this training.

Planning Considerations: The Proposal Stage

Personnel & Staffing

The proposal may seem too early to consider staffing, especially for graduate or postgraduate students. However, it may be critical to assess which personnel may be required to execute the project. Non-U.S. persons may require additional authorizations or licenses prior to being named on the project. If non-U.S. persons are critical to a controlled project, reach out to Research Compliance for advice on what information should be included in the proposal and when Northeastern may need to apply for a license.

It is also worth considering that there may be instances where non-U.S. persons will not be approved for participation. In such cases, you will need to be prepared to identify U.S. persons and/or not participate in the effort.

Hiring may also be slightly more complex. See Appendix B for additional information.

Keep in mind that export-controlled research may limit students' use of this project as a part of their thesis or dissertation. While this research can be a valuable learning experience as part of the graduate students' work, faculty advisors must closely weigh how restrictions (e.g., publication restrictions) will impact students' ability to complete the project and meet academic or graduation requirements. The final publication of the student thesis/dissertation may be embargoed for a certain period of time, or permanently, given the sensitivity of the work

Lab Set-up & Physical Access Controls

When working on restricted research, it is important to keep in mind that only the personnel listed on the TCP should be able to perceive (i.e. see or hear) the controlled activities. That can be as simple as blocking the view to a specific computer screen with a privacy screen or holding meetings in separate rooms with closed doors. We acknowledge that most lab spaces at Northeastern are designed to be open, which may present logistical issues.

For public safety purposes, most spaces at Northeastern have access controls, such as card readers on doors, which log and store access information. If your lab does not have these controls, please work with your college to get a card reader installed.

Even with a card reader to the lab, you may still need to consider additional physical access controls. For example, if your lab has several projects, some controlled and some fundamental, you may need to consider adding storage lockers for controlled materials. Other controls may include implementing a schedule that will provide guaranteed time for controlled project work and fundamental work, as appropriate.

Finally, spaces can be retrofitted to help protect these research activities, including simple fixes like frosting glass, moving computing stations or installing shades.

Any costs that you identify as critical to protecting the controlled research should be raised at the proposal stage. The contract may allow for these costs to be built in, or other sources of support may need to be sought, such as utilizing start-up/discretionary funds or making a request to your college to support such costs.

Research Compliance is available to review proposed research spaces with faculty members to help identify how a space could be secured. Final pricing data will be the responsibility of the PI and college.

Please consider space requirements when preparing a contract or OTA proposal related to a defense agency and if the resulting contract will or could contain CDI. If you do not already have access to one of these spaces, contact Research Compliance to discuss prior to proposal submission.

Secure Account Set-up

All personnel named on a TCP (aside from those in the support category) will require access to a GCC account to store their work and communicate about any controlled projects they may be working on. GCC accounts may be requested by either the PI, individual project team member or college administrator through Service Now. Upon logging into Service Now, search for *GCC account request* and complete the form for the required personnel.

GCC account requests will be routed to either the KRI, LLC FSO or Research Compliance for review and approval. Additional documentation or identity proofing may be required prior to granting account access. GCC accounts do not carry a cost to the PI or lab.

Computing Costs

As mentioned in the section defining GCC and secure computing clusters, there may be costs associated with heavy data processing either through Research Computing's secure computing cluster or standing up your own lab cluster. The costs of these services during and after the project should be evaluated against funding agency guidelines for data retention and sharing to evaluate which costs may be charged directly to the project.

Visitors

At Northeastern, the norm is for labs to be open venues for academic exchange. However, when export-controlled research is conducted in a lab space, it must be protected from access. Only the authorized personnel listed on the TCP should be permitted to participate in or have access to the controlled information or technology.

The TCP will outline procedures for the lab to secure the controlled materials and technology before, during and after use.

Lab Walk-throughs

Northeastern performs screenings on those participating in formal visits. If the TCP is followed, there should be no issues. If you have concerns about a specific delegation or visit, please contact Research Compliance.

Visiting Scientists (both U.S Persons and non-U.S. Persons)
Frequently, faculty members invite visiting scientists to their lab, often for prolonged periods to perform research and collaborate. All visiting scientists should be screened in accordance with Northeastern procedures before they are given access to Northeastern resources. As long as the TCP is followed, no additional action is required unless the PI suspects a breach (steps for reporting breaches are outlined below).

However, in some instances, a faculty member may sponsor a visiting scientist who represents an elevated risk of export control or sanctions violations occurring during the visit. In such instances, Research Compliance may require a Technology Monitoring Plan, with physical and information security restrictions with which the sponsoring faculty, department, and the foreign national visitor must comply.

Unauthorized Visitors
At Northeastern, any unauthorized visitors to your lab should be reported in accordance with the physical breach section below.

KRI, LLC's Security Office may be required to report unauthorized visitors as suspicious contacts to cooperating federal counterintelligence agencies in accordance with NISPOM 1-301 and 1-302(b).

Action plan for suspected breaches

Physical Breach

If you suspect a physical breach, the first step is to contact Research Compliance via researchcompliance@northeastern.edu or the specific individuals named in your TCP, including the Export Control and Logistics Analyst and the Research Security Officer.

Cybersecurity Threat

The first and most critical step is to notify the university by contacting the Office of Information Security (OIS) via ois@northeastern.edu or by phone 617-373-HELP, as well as Research Compliance: researchcompliance@northeastern.edu, and if related to KRI, the KRI FSO at m.cawley@kri.neu.edu. After completing the initial notification, please follow the steps outlined in the University policy on data breaches.

Irrespective of the type of breach, Research Compliance and OIS will work with you to secure the lab, limit the scope of the breach, and ensure any required reports to the funding agency are filed.

Additional Responsibilities

These responsibilities are listed on the Technology Control Plan template and additional information on publication, transfer, amendment to a TCP, reporting requirements, annual reviews, monitoring, audits, and incident notification.

Contacts & Resources

Contacts

Research Compliance: researchcompliance@northeastern.edu
University Compliance: compliance@northeastern.edu
KRI FSO: m.cawley@kri.neu.edu
Research Computing: rchelp@northeastern.edu
OIS: ois@northeastern.edu

Resources

Northeastern Policy on Export Control
Northeastern Export Control Manual
Northeastern Policy on Openness in Research (does not apply to KRI)
Research Compliance Export Control Website
NIST Special Publication 800-171
Bureau of Industry & Security Commerce Control List
Department of Treasury Office of Foreign Asset Control
Directorate of Defense Trade Controls U.S. Munitions List
Department of Energy EINEMR and AFAEAR

Appendix A

Sample Technology Control Plan Data Security Guidelines

All TCPs address how physical and digital work area(s) will be segregated to prohibit unauthorized access to export-controlled material/data.

Best practices include:

1. Identifying a gatekeeper for data access: name a specific individual responsible for adding and removing access to any data covered by the TCP.
2. Specify how data will be accessed, such as:
    a. *Requirements to use secure computing instances provided by Northeastern or KRI, LLC;*
    b. *Applicable prohibitions on downloads or removing computing devices from a specific work location;*
    c. *Restrictions on accessing or downloading data outside of the U.S.; and*
    d. *Steps personnel must take to secure the data when using a shared workstation/computer, such as ensuring no data was accidentally transferred to the desktop or remains in an accessible part of the desktop, where another user could access it.*
3. Describe any applicable measures to segregate the physical workplace, such as:
    a. *Physical security at the lab consists of access-controlled doors and the lab can be separated into publicly accessible and EAR/ITAR controlled areas with signs posted restricting access to approved persons only. Also address how the measure will be enforced, i.e., by personnel or key-card access.*
    b. *Processing in this environment requires lab lock down: this means only U.S. persons may be present in the lab during working sessions. Even if a non-U.S. Person simply walks past a computer, it will be considered transferring that information to them. All personnel on this TCP must ensure non-U.S. persons are not present during project work.*
4. Specifying expectations for all personnel assigned to the project, such as: *assigned personnel may not discuss data or project work with non-U.S. persons. U.S. persons are U.S. Citizens, U.S. permanent residents (green card holders) or asylum seekers. All other persons are considered non-U.S. persons.*

Appendix B

Sample Job Posting Language

As part of its commitment to an open and inclusive environment, Northeastern encourages the use of language that encourages all applicants while also setting forth the expectations of the position. This includes controlled projects that restrict access. We offer the following sample of language that is appropriate to include in a job description for a position tied to an export-controlled project:

To conform to U.S. export control regulations [or for CUI: access requirements stated by the U.S. federal government for this project], applicant should be eligible for any required authorizations from the U.S. Government.

Or

Candidate has capacity to comply with the federally mandated requirements of U.S. export control laws [or for CUI: access requirements stated by the U.S. federal government for this project].

This text is taken from a Sheppard Mullin hiring post, available here.