COGR℠

Advancing Effective Research Policy

Research Security Regulations: Practical Considerations for Technology Transfer Professionals

November 20, 2025

This Guidance is provided as a tool to the COGR Membership with the understanding that COGR is not providing legal, regulatory, or policy advice.

Acknowledgments

Thank you to the Research Security & Intellectual Property Committee (RSIP) for their contributions to the completion of this paper. A special thank you to the following RSIP members:

Hannah Carbone, Director for Innovation, Patents, and Licensing, California Institute of Technology

Elizabeth Peloso, Associate Vice Provost of Research Services, University of Pennsylvania

Bruce Morgan, Associate Vice Chancellor, Research Administration, University of California, Irvine

Allen DiPalma, Executive Director, Office of Research Security & Trade Compliance, University of Pittsburgh

Michael Moore, Director, Technology Transfer, Augusta University

Tom Burns, Associate Vice Provost for Research, Johns Hopkins University

Executive Summary

This guidance provides an overview of the key federal regulations and frameworks pertaining to research security that COGR has identified as most relevant to the work of the technology transfer professional. It highlights both policy expectations and practical considerations for integrating research security into patenting, licensing, and other commercialization activities. The intent is to help technology transfer professionals balance their universities' longstanding commitment to open scientific exchange with increasing federal requirements to safeguard sensitive research outputs, including materials, data, and intellectual property, from unauthorized access, diversion, or foreign exploitation.

Regulatory areas addressed include:

- **Disclosure and Transparency Requirements**: Institutions must report foreign gifts and contracts under Section 117 of the Higher Education Act, with new enforcement provisions established under Executive Order 14282 ("Transparency Regarding Foreign Influence at American Universities"), and disclose significant foreign support through NSF's Foreign Financial Disclosure Reporting requirement. TTOs must track licenses and other revenue-generating agreements with foreign entities to ensure timely and accurate institutional reporting.
- **Fundamental Research and Export Control**: National Security Decision Directive 189 defines fundamental research as research whose results are ordinarily published and broadly shared within the scientific community, and thus generally exempt from export control restrictions under the fundamental research exclusion. However, once research transitions from open academic inquiry to activities involving proprietary development or commercialization, this exemption from export controls no longer applies in many cases.

  Compliance with the International Traffic in Arms Regulations, Export Administration Regulations, and other trade compliance regulations is essential to ensuring that controlled technologies, technical data, and software are not improperly transferred or disclosed to unauthorized parties. TTOs play a key role in this process by adhering to institutional export control procedures during licensing, material transfer, and data access activities. Through coordination with the university's export control officer, TTOs help ensure that each transaction is reviewed for potential export restrictions so that appropriate export licenses are in place when necessary.
- **Restricted Information**: Controlled Unclassified Information and Federal Contract Information are subject to specific information protection and cybersecurity requirements and must be safeguarded in accordance with

established federal frameworks. TTOs play a critical role in managing these obligations, particularly when transferring or otherwise sharing such restricted information. Access must not be granted without explicit authorization from the controlling federal agency, and restrictions apply even when sharing with collaborators, subcontractors, or licensees. To mitigate risk and ensure compliance, TTOs should maintain close coordination with sponsored programs administrators, compliance personnel, and the relevant sponsoring agency. This collaboration helps confirm that any transfer or dissemination of restricted information aligns with contractual obligations and federal regulations.

- **Sensitive Information Transfers**: The Department of Justice's Data Security Program and the National Institutes of Health's Notice of Enhanced Security Measures for Human Specimens establish heightened standards for the secure transfer and management of sensitive datasets and biospecimens. These frameworks require institutions to conduct enhanced due diligence on recipients and their locations, verify that partner organizations have the capacity to safeguard controlled access of sensitive materials, and include explicit data protection provisions in data use agreements and material transfer agreements. For TTOs, these requirements underscore the importance of integrating research security and cybersecurity considerations into data and material transfer processes to ensure compliance with federal expectations while supporting responsible research collaborations and commercialization.
- **Patents and Foreign Filings:** Foreign patent protection can introduce research security considerations for TTOs, particularly when inventions arise from federally funded research. Filing in foreign jurisdictions may involve technical data that requires review for export control, foreign participation, or national security sensitivities. TTOs and researchers also need to be aware that, when submitting proposals to the Department of Defense, any federally funded patents or patent applications filed first in a country of concern, or on behalf of an entity connected with a country of concern, must be disclosed to the agency and may prompt a request for a mitigation plan. Through close coordination with export control officers and patent counsel, TTOs can ensure that foreign filing strategies, inventor participation, and patent prosecution activities are evaluated for potential risks, while supporting the responsible protection and commercialization of university innovations.
- **Foreign Investment and CFIUS**: The Committee on Foreign Investment in the United States, strengthened under the Foreign Investment Risk Review Modernization Act, has expanded authority to review non-controlling foreign investments in university-affiliated startups developing critical or export-

controlled technologies. For TTOs, this expansion could have implications for managing and structuring startup licenses. TTOs should coordinate with the university's general counsel to determine the appropriate level of due diligence when licensing to a startup.

Collectively, the requirements highlighted in this document underscore the expanding role of technology transfer professionals in research security, as they serve as stewards of intellectual property and innovation. By embedding research security compliance awareness into the TTO's operations, technology transfer professionals ensure that their universities' research outcomes are transferred for public benefit in a manner consistent with federal research security requirements. Through collaboration with sponsored programs administrators, research security professionals, export control officers, information security professionals, and general counsel, TTOs enable the university to maintain both its research integrity and its eligibility for federal funding while strengthening its position as a trusted and responsible research partner.

Table of Contents

Introduction

Technology Transfer Offices (TTOs) play a vital role in the university's mission to advance innovation, protect intellectual property (IP), and translate research discoveries into societal and economic benefit. Through licensing, the transfer of data and materials, and startup formation, TTOs help ensure that the results of federally funded research contribute to technological progress and public value. However, in today's complex geopolitical and regulatory environment, technology transfer professionals are increasingly being called upon to serve as stewards of research security, helping protect the research enterprise from risks posed by malign foreign influence, IP theft, data misuse, and noncompliance with federal requirements.

The U.S. Government has made research security a national priority, emphasizing the need for consistent institutional standards across the academic community. Through National Security Presidential Memorandum (NSPM)-33, its implementation guidance, and subsequent agency-specific policies, federal sponsors have directed universities to strengthen internal controls around disclosure, cybersecurity, export compliance, and foreign engagement. These measures aim to preserve the integrity of the U.S. research ecosystem while ensuring that federally funded innovations remain secure from unauthorized exploitation or diversion. As detailed in this document, this evolving regulatory landscape has direct and practical implications for TTOs.

Awareness of research security requirements is no longer peripheral to technology transfer operations. In this environment, TTOs occupy a strategic intersection between compliance, innovation, and national security. Offices are being asked to balance the university's commitment to open scientific exchange with its obligation to safeguard sensitive technologies and research data. Doing so requires close coordination with research compliance offices, export control specialists, research security professionals, general counsel, information security teams, and sponsored programs administrators. By integrating research security considerations into every stage of the technology transfer process, from materials and data sharing to invention disclosure and patent filing to licensing and commercialization, TTOs help ensure that innovation proceeds responsibly and securely, in alignment with both institutional values and federal expectations.

While this document highlights key federal regulations and frameworks, it is not an exhaustive summary of all research security regulatory requirements. Instead, it presents a focused overview of the most relevant functions and responsibilities of TTOs, emphasizing the areas where compliance, research integrity, and commercialization activities intersect most directly.

Institutional Disclosure Requirements

Universities and their researchers share a collective responsibility to disclose sources of research support (current and pending support), foreign affiliations, and participation in foreign talent recruitment programs, in accordance with federal requirements. Failure to accurately disclose external commitments or affiliations can compromise federal funding, result in administrative or civil penalties, and call into question ownership of IP. While TTOs do not have formal responsibility for many of these disclosure requirements, they do play a supporting and compliance-adjacent role in ensuring that institutional obligations under the Department of Education's Section 117 (Section 117) requirements and the National Science Foundation's Foreign Financial Disclosure Reporting (FFDR) requirements are met.

Section 117 Foreign Gift and Contract Reporting. Under Section 117 of the Higher Education Act, U.S. colleges and universities are required to report twice yearly to the Department of Education (Dept of Ed) any foreign gifts or contracts valued at $250,000 or more, either individually or in combination, from a single foreign source in a calendar year. The regulation applies broadly to funds, services, property, and in-kind support, and institutions must provide detailed disclosure of the terms, source, and purpose of such arrangements. In April 2025, Executive Order 14282, "Transparency Regarding Foreign Influence at American Universities," intensified enforcement of these reporting obligations by directing the Dept of Ed to take stronger action to ensure full disclosure, require institutional certifications of compliance, and invoke penalties under the False Claims Act for institutions that knowingly misstate or conceal material information.

NSF Foreign Financial Disclosure Reporting (FFDR). The National Science Foundation (NSF) has implemented the FFDR requirement to strengthen transparency around foreign support and affiliations of NSF-funded researchers. Under this policy, each institution of higher education that receives NSF funding must disclose annually any financial support with a cumulative value of $50,000 or more received from an entity associated with a country of concern. Core countries of concern are the People's Republic of China, the Democratic People's Republic of Korea, the Islamic Republic of Iran, and the Russian Federation.

Practical Considerations for TTOs:

- Implement a system to identify and track all agreements (licenses, material transfer agreements (MTAs), data use agreements (DUAs), etc.) it negotiates with foreign parties involving any form of consideration.
- In collaboration with the institution's empowered official or designated reporting officer ("Responsible Party"), develop and document a methodology

to assign monetary value to such consideration as equity, in-kind support, and any other non-cash consideration.

- Since the Section 117 threshold is $250,000 for all transactions across the institution with a single foreign source, work with the Responsible Party and other stakeholders to identify which office is responsible for aggregating and reporting the total transactions by source.
- Confirm with the Responsible Party what specific information the TTO must collect and when such information needs to be submitted. At a minimum, TTOs should expect to provide: the name and the principal place of business of the foreign source, the value of the contract and the type of agreement. Reports for Section 117 are due biannually on January 31 and July 31. NSF FFDR reports are due July 31.
- The definitions of "foreign source" (under Section 117) and "country of concern" (under NSF FFDR) include agents, subsidiaries and affiliates of foreign entities. TTOs should work with the Responsible Party to establish and document a procedure for identifying affiliated foreign entities and determining when such entities fall within the scope of reporting obligations.
- TTOs should develop a procedure to ensure consistent recording of names of foreign entities and their principal place of business. The use of standardized naming conventions across agreements and databases will support data integrity and prevent duplication or reporting errors.

Fundamental Research and Export Control

Export control laws, including the Department of State International Traffic in Arms Regulations (ITAR) and the Department of Commerce Export Administration Regulations (EAR), govern the export and reexport of certain commodities, technologies, technical data, software, and services to foreign entities, whether those transfers occur through physical shipment, electronic transmission, or even oral or visual disclosure (including to non-U.S. persons located within the boundaries of the U.S., known as a "deemed export"). These regulations are designed to protect U.S. national security and foreign policy interests by controlling access to items that could contribute to the military or strategic capabilities of foreign nations.

A critical distinction for universities is that most campus-based research is intended to fall under the fundamental research exclusion (FRE). This distinction was first articulated in the National Security Decision Directive (NSDD) -189 and subsequently recognized within both the ITAR and the EAR. Under this exemption, the results of basic and applied research that are ordinarily published and broadly shared within

the scientific community are not subject to export controls, provided that no publication or foreign national access restrictions are imposed by the sponsor or through contractual terms. However, when research involves proprietary or restricted data, controlled technology, or sponsor-imposed dissemination limits, it falls outside the scope of the FRE and may trigger additional export control obligations.

Issued in 1985 and reaffirmed by multiple administrations, NSDD-189 establishes the national policy on the transfer of scientific, technical, and engineering information produced through federally funded research. It defines fundamental research as "basic and applied research in science and engineering, the results of which are ordinarily published and shared broadly within the scientific community." The directive explicitly states that to the maximum extent possible, the results of fundamental research should remain unrestricted. This policy remains the cornerstone of the U.S. approach to open scientific exchange and innovation. It balances the nation's need to protect sensitive technologies with the equally vital goal of preserving the open academic environment that drives discovery and economic growth.

For universities, NSDD-189 provides the foundation that distinguishes open academic research from controlled research subject to export controls and federal data protection standards. Research results designated as fundamental fall under the FRE, meaning the results are not controlled by either EAR or ITAR. This distinction helps maintain the free exchange of ideas, supports international collaboration, and enables education involving foreign graduate students and postdoctoral researchers. It should be noted that the FRE only applies to technology (i.e., data and other intangible outputs generated under a research project) and some software that arises from fundamental research. The exclusion does not apply to commodities, prototypes, and other tangible products.

In many cases, innovations resulting from fundamental research can be broadly marketed and licensed by the TTO without the need for an export control determination, clauses related to restricted data handling, or access and facility controls, provided that the research results are publicly available or intended for publication. Once research transitions from the stage of open academic inquiry to applied development, commercialization, or licensing activities, however, the FRE may no longer apply. For example, a license granting rights to the claims of a published patent only will be afforded the benefits of the FRE. However, a license that includes the rights to underlying, proprietary know-how or any other results not disclosed in the patent application, or otherwise made available to the scientific community, can narrow or eliminate the benefits of the FRE.

Practical Considerations for TTOs:

- Verify that research outputs being transferred under a license agreement, DUA, MTA, collaboration, or other agreement are the results of fundamental research and not controlled technical data or information subject to export controls.
- Ensure terms of sponsored research agreements, any affiliated non-disclosure agreements (NDAs), and any subsequent license agreements do not impose publication or access restrictions that would unintentionally negate the benefits of the FRE.
- Confirm that the appropriate compliance office (likely the export control office) has evaluated the prospective third party against U.S. restricted party lists and "Know Your Customer" guidance from the Department of Commerce to identify and manage any identified high-risk elements in the transaction.
- In accordance with your university's practice, request the institutional export control staff to assess technology jurisdiction and classification before transferring materials, data, or software.
- Consider including language in licenses, DUAs, MTAs, and other such agreements requiring the counterparty to abide by U.S. export control laws, as applicable, and to confirm that it is not a restricted party, or otherwise subject to U.S. trade sanctions or restrictions.
- Include a copy of the export review determination or any guidance provided by the export control staff in the license file.

Requirements for Restricted Information

As research transitions from open publications to more restricted activities involving federally controlled or contractually restricted information, different compliance obligations arise. Universities handling Controlled Unclassified Information (CUI) or Federal Contract Information (FCI) must comply with security frameworks such as NIST Special Publication 800-171 and Cybersecurity Maturity Model Certification (CMMC) requirements. CUI refers to non-classified U.S. government information, including information generated on behalf of the government, that requires safeguarding or dissemination controls pursuant to federal laws, regulations, or government-wide policy. This includes certain data, technical information, or export-controlled materials associated with federally funded research. FCI encompasses information not intended for public release that is provided by or generated for the federal government under a defense contract.

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (NIST SP 800-171). NIST Special Publication (SP) 800-171, titled *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, establishes the baseline cybersecurity requirements for any nonfederal organization—including universities, research institutions, and contractors—that stores, processes, or transmits CUI on behalf of the U.S. government. CUI may include research data, technical specifications, export-controlled information, personally identifiable information (PII), or other materials associated with federal contracts, grants, or cooperative agreements.

The NIST SP 800-171 framework defines 110 security requirements organized into 14 control families: access control, awareness and training, audit and accountability, configuration management, identification and authentication, incident response, maintenance, media protection, personnel security, physical protection, risk assessment, security assessment, system and communications protection, and system and information integrity. Together, these controls provide a comprehensive approach to safeguarding sensitive federal data in nonfederal environments, ensuring that it remains protected from loss, unauthorized disclosure, or compromise.

For higher education and research institutions, compliance with NIST SP 800-171 is increasingly relevant as federal agencies expand requirements for protecting sensitive information shared through research collaborations and sponsored projects. Discussed in more detail below, the Department of Justice's Sensitive Data Program and the NIH's Notice NOT-OD-25-160 both reference NIST SP 800-171 as the benchmark for verifying that third-party recipients or collaborators maintain appropriate information security capabilities. Institutions that handle controlled-access datasets, sensitive personal data, or federally funded research materials may therefore be required to demonstrate that their information systems and practices align with NIST's prescribed standards.

Cybersecurity Maturity Model Certification Program. The Cybersecurity Maturity Model Certification (CMMC) Program is a Department of Defense (DOD) initiative designed to ensure that all defense contractors and subcontractors maintain an adequate level of cybersecurity to protect CUI and FCI handled in the performance of DOD contracts. Initially introduced in 2020 and refined under the CMMC framework implemented in 2025, the program integrates existing cybersecurity standards into a unified compliance model that applies across the Defense Industrial Base, including universities, research institutions, and laboratories that perform research or provide services under DOD-funded contracts.

CMMC provides a tiered framework of cybersecurity maturity levels that reflect increasing levels of protection and assurance. Under CMMC, there are three

certification levels. The level of certification required depends on the nature of the contract and the type of information being accessed or generated. All entities within the DOD supply chain (whether prime contractors or subcontractors) must implement the required cybersecurity controls for their designated level and may be subject to third-party or government assessments to verify compliance before contract award or continuation.

TTOs must exercise heightened diligence when handling the transfer or sharing of CUI and FCI obtained or generated through federally sponsored projects. Both categories of information are subject to specific federal requirements governing their dissemination, access, and protection. Unauthorized transfers can result in violations of contractual obligations, federal regulations, and institutional policy.

CUI may not be disclosed or transferred to any third party unless such transfer is explicitly authorized in writing by the federal agency that owns, originates, or controls the information. Authorization typically occurs through contract provisions, DUAs, or agency correspondence that define approved recipients and permissible uses of the data. In the absence of such approval, CUI must remain secure within the institution-controlled research environment and may not be released externally, even to collaborators, industry partners, or subcontractors. Any authorized transfer must be accompanied by appropriate security assurances, ensuring that the recipient organization has demonstrated capability to protect CUI in accordance with NIST SP 800-171 and other applicable federal information protection standards.

FCI may be shared with a third party only when such sharing is necessary for the performance of the contract under which the FCI was originally provided or generated. This means that access to FCI must be limited to subcontractors, collaborators, or other service providers who have a legitimate need for the information to fulfill contractual obligations and who are bound by written agreements to implement equivalent security and confidentiality protections. The sharing of FCI for purposes outside the scope of the prime contract, such as general collaboration, publication, or commercialization, requires prior approval from the contracting officer or relevant federal agency authority.

Practical Considerations for TTOs:

- Treat any data marked or otherwise designated as CUI or FCI as restricted for dissemination. Data generated during the performance of a project under a contract or subcontract that is not considered fundamental research should also be treated as restricted until confirmed otherwise with the appropriate compliance office or the federal agency funding the research. (NOTE: A federal contract normally supports fundamental research if it (i) allows for unfettered publication of the results and (ii) does not contain any CUI, classified information, or other restrictive national security related clauses.)

- Do not transfer CUI unless the transfer to the receiving party is explicitly authorized by the federal agency that owns or controls such information.
- Work with general counsel and the appropriate compliance offices to ensure institutional NDAs and DUAs incorporate required data security language for CUI and FCI, including audit rights and restrictions on both data use and additional dissemination of the data to third parties.
- CUI should not be included in patent applications. It may be possible that, in coordination with the Principal Investigator, all controlled data can be generalized such that CUI is omitted. It is important to work with the appropriate compliance office and/or the sponsoring agency to ensure all materials contained in a patent application are fully sanitized and publicly releasable prior to submitting to the USPTO.

Other Restrictions on Sensitive Information Transfers

The U.S. Government is placing increasing emphasis on the responsible and secure management of sensitive datasets and biological materials, particularly those that contain personally identifiable information (PII), controlled-access data, or research materials with national security or law enforcement implications. Federal policy reflects growing concern over the potential misuse, theft, or unauthorized transfer of such information and materials by foreign entities or other actors who may pose risks to U.S. interests. This evolving policy landscape requires universities, research institutions, and their collaborators to implement stronger safeguards and enhanced due diligence when engaging in activities that involve the sharing or transfer of federally funded data or biospecimens.

Two key federal requirements that TTOs need to be aware of are the Department of Justice's Data Security Program (DSP) and the National Institutes of Health's Notice NOT-OD-25-160: NIH Policy on Enhancing Security Measures for Human Biospecimens.

Department of Justice (DOJ) Data Security Program (DSP). The DOJ DSP, codified in 28 CFR Part 202, establishes federal standards for the protection, management, and transfer of sensitive datasets generated, accessed, or held by federally funded institutions. This regulation implements key provisions of Executive Order 14117, "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern," which seeks to prevent foreign adversaries and other unauthorized actors from accessing large volumes of U.S. persons' sensitive personal data. The DOJ DSP applies broadly to any federally funded research or administrative activity involving sensitive or controlled datasets,

including those derived from human subjects research, national security–related data, or other forms of PII.

Under the DOJ DSP, universities and other federally funded entities are required to conduct enhanced due diligence before sharing sensitive datasets with any third party, domestic or international. This includes assessing the recipient organization's ownership, control, and affiliations to ensure that it is not directly or indirectly linked to countries of concern or entities subject to U.S. national security restrictions. Institutions must also incorporate contractual assurances in DUAs, Data Access Agreements (DAAs), or similar research collaboration instruments confirming that the recipient has the technical and organizational capacity to protect sensitive data consistent with federal standards.

A central requirement of the DOJ DSP is that recipients maintain cybersecurity and access controls that meet or exceed federal information protection frameworks such as NIST Special Publication 800-171 for any data subject to the DSP requirements. Institutions must verify and document that third-party partners have implemented appropriate controls for access restriction, encryption, monitoring, and incident response. Agreements should further require that data recipients comply with all applicable U.S. export control and data security regulations, promptly report any data breaches or unauthorized access, and submit to audits or oversight when requested by the data provider or a federal agency.

The program also requires that all agreements prohibit unauthorized dissemination or downstream transfer of sensitive data. Data may not be re-shared, sublicensed, or made available to additional entities or personnel beyond those explicitly approved in the governing agreement. Any proposed subsequent transfer or collaboration involving the data must undergo a new due diligence review and approval process.

Institutions are responsible for maintaining detailed records of such reviews, agreements, and any approved exceptions, and must be prepared to produce this documentation upon request to federal agencies.

National Institutes of Health NOT-OD-25-160. NIH Notice NOT-OD-25-160, effective October 24, 2025, establishes new security expectations for the management, use, and transfer of human biospecimens and other sensitive research materials derived from U.S. persons. The policy aligns NIH requirements with recent federal directives, including Executive Order 14117 and the DOJ DSP, which seek to prevent unauthorized foreign access to bulk sensitive personal data and related materials. The guidance applies to all NIH-funded activities involving the collection, storage, use, or distribution of human biospecimens—whether identifiable or not—and extends across all NIH funding mechanisms, including grants, cooperative agreements, contracts, and intramural research.

Under NOT-OD-25-160, NIH explicitly prohibits the transfer or sharing of covered biospecimens with entities or individuals located in countries of concern, except under narrowly defined circumstances. Exceptions may be granted only when required by U.S. law or formal international agreements, when a unique foreign collaborator possesses capabilities unavailable elsewhere and the transfer is fully justified and documented, or when the transfer occurs at the request of a donor for their own medical benefit and in accordance with U.S. laws and informed consent. Institutions are expected to maintain detailed documentation of all transfers and any exceptions, and to produce such records upon NIH request.

Under NOT-OD-25-160, NIH also updated its expectations for the use of DUAs and MTAs involving controlled-access datasets, biospecimens, or other sensitive research materials. These agreements must now explicitly confirm that recipient institutions possess the technical and administrative capacity to protect such materials in accordance with NIH security requirements. The DUA or MTA should affirm that the recipient has implemented adequate data and material security controls—such as secure environments, access monitoring, and restricted sharing—and that the recipient agrees to comply with all relevant NIH policies governing data and biospecimen security.

Additionally, DUAs and MTAs must incorporate terms that prohibit the further transfer of covered materials to countries of concern or to entities affiliated with them, unless a permitted exception applies.

TTOs play a central role in ensuring agreements include clear data security language, align with institutional policies, and define responsibilities for storage, use, and disposition of transferred materials in accordance with the evolving federal regulatory environment.

Practical Considerations for TTOs:

- Work with general counsel and compliance offices to ensure institutional MTAs and DUAs incorporate DOJ- and NIH-required data security language, including audit rights and restrictions on downstream sharing.
- Before approving transfers of sensitive data or biological materials, confirm that the recipient institution has adequate data protection controls, storage capacity, and compliance certifications, in accordance with your institution's practice.
- Provide guidance to investigators about the use of MTAs or DUAs and when such agreements are required.

- Maintain clear records of data and material transfers to demonstrate compliance with DOJ program requirements and NIH's oversight expectations.

Patents and Foreign Filings

When a university seeks patent protection outside the United States for an invention arising from federally funded research, it must first comply with U.S. export control and patent security requirements. Under 37 CFR Part 5, before a U.S. invention may be filed abroad, the applicant must obtain a foreign filing license from the USPTO.

A foreign filing license is either granted automatically upon filing a U.S. patent application or issued separately upon request if a TTO intends to file abroad before a U.S. application is submitted. The USPTO conducts a national security review, in coordination with other federal agencies, to determine whether the invention or its underlying technology could affect national defense or foreign policy interests. If potential national security concerns are identified, the USPTO can impose a secrecy order under 35 U.S.C. § 181, restricting the publication or foreign filing of the invention until the order is lifted.

Once a license is granted, the TTO may proceed with foreign patent filings through mechanisms such as the Patent Cooperation Treaty (PCT) or direct national filings in individual jurisdictions. A foreign filing receipt is then issued, confirming that the application has been officially filed in the foreign country or through the PCT system.

Foreign Patents and the DOD Component Decision Matrix to Inform Fundamental Research Proposal Mitigation Decisions. The Department of Defense decision matrix establishes a standardized, risk-based framework for assessing potential national security concerns associated with proposed fundamental research projects. The matrix is used by DOD program managers to identify whether a researcher's affiliations, funding sources, or activities create unacceptable or mitigable risks to determine whether mitigation is required or the proposal must be disqualified. Mitigation measures may include enhanced disclosure requirements, restrictions on foreign collaboration, or substitution of key personnel.

In addition to evaluating participation in foreign talent recruitment programs, funding from foreign countries of concern, and affiliations with entities on U.S. restricted party lists, the matrix specifically includes the assessment of foreign patenting activities of key personnel as a potential indicator of risk. For patents or patent applications listed in the proposal that resulted from federally funded research, the DOD requires institutions to develop a mitigation plan if such patents or applications were filed in a country of concern, or on behalf of an entity within a

country of concern, prior to their filing in the United States. DOD also recommends that institutions prepare a mitigation plan whenever a disclosed patent or patent application has any nexus to a country of concern, involves a foreign co-inventor or assignee with restricted affiliations, or raises potential conflicts under U.S. export control laws.

Practical Considerations for TTOs:

- Confirm that the USPTO has granted a foreign filing license before filing a patent application in another country. If filing non-domestically before a U.S. application is submitted, obtain an explicit license under 37 CFR Part 5. Document rationale for filing a foreign patent application prior to filing a U.S. application. Criteria for when a foreign filing license is not required can be found at the USPTO's MPEP 1832.
- Collaborate with export control officers to screen third parties and to determine if the draft application contains CUI or export-controlled technical data prior to any foreign filings and coordinate with counsel to determine whether redactions or claim modifications are necessary.
- Engage with university counsel to review and update inter-institutional agreement templates to address notification and consent of patent filings in foreign jurisdictions.
- Work with university counsel to determine under what circumstances, if any, the TTO may delegate patent prosecution authority under a license agreement and to what extent a licensee may control the patent prosecution process.

Foreign Investment and University Startups

The Committee on Foreign Investment in the United States (CFIUS), an interagency body chaired by the U.S. Department of the Treasury, reviews certain transactions that could result in foreign control or influence over U.S. businesses to determine whether they pose national security risks. The Foreign Investment Risk Review Modernization Act (FIRRMA) significantly expanded CFIUS authority beyond traditional mergers and acquisitions to include non-controlling, minority investments in companies engaged in critical technologies, critical infrastructure, or the collection and use of sensitive personal data.

For TTOs, this expanded scope is important. Many university-affiliated startups are formed around IP in technical fields that are export controlled under the EAR or

ITAR. Examples include innovations in semiconductors, AI, quantum computing, cybersecurity, advanced materials, energy storage, and biotechnology.

Under FIRRMA, even a small foreign equity investment or a research collaboration that provides a foreign entity with access to technical information, board representation, or decision-making rights can trigger a CFIUS "covered transaction" review. This means that TTOs and university-affiliated venture funds must exercise heightened diligence when facilitating or approving startup investments or license agreements involving foreign investors.

Practical Considerations for TTOs:

- To the extent consistent with your university's policies, work with university-affiliated startups and appropriate university compliance offices to screen the startup's potential investors for foreign ownership, government connections, or links to countries of concern.
- Collaborate with export control officers to determine whether a startup's underlying technology falls within CFIUS jurisdiction (e.g., controlled under the ITAR or EAR).
- Consider including training about CFIUS in the curriculum of campus entrepreneurial programs so university-affiliated founders understand when a CFIUS filing may be mandatory or advisable, and how it might impact fundraising.
- Consider including language in license agreements with university-affiliated startups requiring licensees to abide by CFIUS rules.
- Engage with university counsel to determine the level of due diligence the TTO may need to exercise when equity was issued by a university-affiliated startup as consideration for the license versus when the university does not have an equity position.
- Work with the various campus stakeholders to establish risk tolerance when foreign capital is sought by a startup licensee.

Conclusion

For technology transfer professionals, research security has evolved from a peripheral compliance obligation into a central element of both the university's research and technology transfer missions. As federal expectations for higher education to protect technologies from unauthorized exploitation continue to expand, TTOs now operate at the critical intersection of innovation, compliance, and

national security, helping to ensure that the university's research enterprise remains both open and secure. The contemporary research environment requires TTOs not only to facilitate the dissemination and commercialization of new technologies but also to safeguard those innovations from unauthorized access and diversion.

Integrating research security into technology transfer operations requires a familiarity with the diverse and evolving regulatory frameworks that govern federally funded research as well as the university's own practices and policies. The federal regulatory landscape now encompasses a plethora of requirements that directly and indirectly impact TTOs. Compliance in these areas requires close coordination with export control offices, research compliance units, general counsel, sponsored programs administration, and information security teams, creating a shared institutional responsibility for managing research risk.

Ultimately, a proactive, well-integrated approach to research security enables universities to advance their research missions with integrity and confidence. By embedding security considerations into the daily practice of technology transfer, through due diligence, partner vetting, secure data management, and researcher education, TTOs strengthen institutional resilience, maintain eligibility for federal funding, and protect the long-term value of university-generated innovations.

Appendix A: Additional Resources

BIS Guidance for Deemed Exports

BIS Export Compliance Guidelines

CFIUS Laws and Guidance

COGR's Summary of Guidance for Implementing NSPM Disclosure Requirements

COGR's Foreign Influence on Research – Practical Considerations in Developing an Institutional Response.

COGR's Overview of DOD's CMMC 2.0 Framework

Copy of NSDD-189

Department of Education Section 117 Published Guidance

DOD Chief Information Officer CMMC Resources

DOD Fundamental Research Guidance

DOJ Data Security Program Compliance Guide

NSF Foreign Financial Disclosure Report Applicability and Requirements

Appendix B: Glossary of Terms

Biospecimens –samples of biological material such as blood, tissue, DNA, or protein which are often stored in repositories for later use in research. Human biospecimens also include those samples that are isolated or propagated into new cell lines.

Controlled Unclassified Information (CUI) – unclassified information created by or on behalf of the United States government that requires safeguarding or dissemination controls limiting its distribution to those individuals who have a lawful government purpose to access.

Country of Concern – The core countries of concern for NSF FFDR purposes include the People's Republic of China, the Democratic People's Republic of Korea, the Islamic Republic of Iran, and the Russian Federation. The updated list of countries of concern can be found at 28 CFR 202.601, which adds Cuba and Venezuela to the above list and defines China to include Macau and Hong Kong. It is important to note that the list of "countries of particular concern" is not the same as the list for "countries of concern".

Deemed Export – refers to the release of controlled technologies or technical data to a foreign national within the United States. A deemed export is subject to the same export licensing requirements as other exports.

Export Administration Regulations (EAR) –refers to the set of regulations administered by the U.S. Department of Commerce's Bureau of Industry and Security (BIS) that control the export and re-export of certain goods, software, and technologies.

Federal Contract Information (FCI) – information provided by or generated for the United States government under a contract that is not intended for public release. (See 48 CFR 52.204-21)

Foreign Source – Under the Higher Education Act, Section 117 and the CHIPS and Science Act of 2022 (with respect to NSF FFDR requirements) a foreign source means: (a) a foreign government, including an agency of a foreign government; (b) a legal entity, governmental or otherwise, created solely under the laws of a foreign state or states; (c) an individual who is not a citizen or national of the United States or a trust territory or protectorate thereof; and (d) an agent, including a subsidiary or affiliate of a foreign legal entity, acting on behalf of a foreign source. (See 42 U.S. Code § 19040)

Fundamental Research – See National Security Decision Directive 189 (below).

Fundamental Research Exclusion – an exemption from United States export control laws for basic or applied research in science or engineering, conducted at an accredited institution of higher education within the United States, where the results of the study are ordinarily published and shared broadly within the scientific community.

International Traffic in Arms Regulations (ITAR) - refers to the set of regulations administered by the U.S. Department of State that control the export of defense and military technologies.

National Security Decision Directive (NSDD) – 189 - issued in 1985, the directive defines *fundamental research* as "basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons."

Patent Cooperation Treaty (PCT) Application – an international patent application that allows inventors to seek patent protection in multiple countries by filing a single initial application.

Personally Identifiable Information (PII) – any information that can be used to identify an individual, whether directly or indirectly.

Appendix C: Desk Reference Guide

Research Security Topic	MTA	DUA	License
Institutional Disclosure Requirements (Section 117, NSF FFDR)	Must be tracked if any consideration is received for material transfer to a foreign entity.	Must be tracked if any consideration is received for data transfer to a foreign entity.	Licenses with foreign entities must be tracked for institutional reporting obligations.
Fundamental Research & Restricted Data (NSDD-189, CUI/FCI)	Material transfers may involve restricted data requiring compliance.	Data transfers may involve restricted data requiring compliance.	Licenses may include proprietary know-how beyond published research, triggering export control obligations.
Data Security & Transfer Controls (DOJ DSP, NIH NOT-OD-25-160)	MTAs must include security provisions for biospecimens and sensitive materials.	DUAs must include security provisions for sensitive datasets.	Generally, not applicable unless the license includes transfer of sensitive data or biospecimens.
Export Control & Foreign Engagement (ITAR, EAR, FRE)	Material transfers may require export control review and compliance.	Data transfers may require export control review and compliance.	Licenses often involve technology subject to export controls; compliance is critical.
Cybersecurity Requirements (NIST SP 800-171, CMMC)	MTAs involving CUI/FCI require cybersecurity compliance.	DUAs involving CUI/FCI require cybersecurity compliance.	Rarely applicable unless the license includes access to CUI/FCI.
Foreign Filing & Patent Security (USPTO Foreign Filing License, Secrecy Orders)	Not applicable.	Not applicable.	Foreign patent filings require a USPTO license and may trigger secrecy orders; TTO must ensure compliance.
Foreign Investment & CFIUS (University-affiliated startups)	Not applicable.	Not applicable.	Licenses to startups with foreign investment may trigger CFIUS review; due diligence required.
BIS Affiliates Rule (50% Ownership Standard [1]	*Transfers of materials to foreign affiliates of listed entities may require export control review and compliance.*	*Data transfers to foreign affiliates of listed entities may require export control review*	*Licensing IP to startups or companies with foreign investment now requires ownership screening and, in some cases, BIS licensing.*

[1] *The Affiliates Interim Final Rule implementation has been delayed until October 2026 by the Trump Administration. Please refer to Appendix D for more information about the BIS Affiliates Rule.*

Appendix D: Bureau of Industry and Security Affiliates Rule

On September 30, 2025, the Bureau of Industry and Security (BIS) issued an interim final rule, commonly referred to as the "Affiliates Rule", which requires foreign entities at least 50% owned by one or more sanctioned parties on certain U.S. restricted party lists to be subject to the same export restrictions as their majority owners. If a license or collaboration involves transferring controlled technical data or materials to an entity covered under the Affiliates Rule, an export license may be required even if the originating research was fundamental or the licensee is incorporated in a non-restricted country. It is important to first understand the export restrictions that apply to the majority owners before determining whether an export license is required for a license or collaboration.

U.S. affiliates of foreign entities designated under the rule, however, are expressly exempt from its restrictions, even if the affiliate would otherwise meet the criteria for inclusion. In other words, a U.S.-incorporated subsidiary or affiliate of a listed foreign entity is not automatically subject to the same licensing or export control requirements solely by virtue of its ownership or corporate relationship.

Effective November 10, 2025, BIS suspended the rule for a period of twelve months. The suspension will end on November 9, 2026, unless further extended by the Administration.

The final implementation of the Affiliates Rule will impose a significant burden on the appropriate compliance office in evaluating the prospective third party, as the entity will not necessarily be named on U.S. restricted party lists. However, the principles of the "Know Your Customer" guidance from the Department of Commerce, to identify and manage high-risk elements in a transaction, still apply. A TTO's obligation to confirm that the appropriate compliance office has completed an evaluation will remain unchanged.