BOISE STATE UNIVERSITY

University Policy 5120

Export Control and Controlled Data

Effective Date

August 04, 2023

Responsible Party

Division of Research and Economic Development, (208) 426-5732

Scope and Audience

This policy applies to all university personnel including faculty, staff, visiting scholars, student employees, students, affiliates, and volunteers.

Additional Authority

- Arms Export Control Act ("AECA")
- International Emergency Economic Powers Act ("IEEPA")
- Export Control Reform Act ("ECRA")
- International Traffic in Arms Regulations ("ITAR")
- Export Administration Regulations ("EAR")
- Office of Foreign Assets Control ("OFAC")
- 10 CFR Part 110 Export and Import of Nuclear Equipment and Material
- 10 CFR Part 810 Assistance to Foreign Atomic Energy Activities
- 32 CFR Part 2002 Controlled Unclassified Information ("CUI")
- Family Educational Rights and Privacy Act ("FERPA")
- Health Insurance Portability and Accountability Act ("HIPAA")
- National Institute of Standards and Technology ("NIST")
- Idaho State Board of Education Institution Technology Licensing Guidelines
- University Policy 1020 (Public Records Management)
- University Policy 1090 (Intellectual Property)

- University Policy 1110 (Conflict of Interest and Commitment)
- University Policy 1150 (HIPAA Hybrid Entity Designation)
- University Policy 6180 (Travel)
- University Policy 8000 (Information Technology Resource Use)
- University Policy 8060 (Information Privacy and Data Security)

1. Policy Purpose

To provide guidance regarding U.S. laws and regulations related to export control and controlled data.

2. Policy Statement

Boise State University is committed to fully complying with all U.S. laws and regulations related to export control and controlled data

3. Definitions

3.1 Person

A natural person as well as a corporation, business association, partnership, society, trust, or any other entity, organization or group, including governmental entities.

3.2 U.S. Person

A person who is a lawful permanent resident as defined by 8 U.S.C. 1101(a)(20) or who is a protected individual as defined by 8 U.S.C. 1324b(a)(3). It also means any corporation, business association, partnership, society, trust, or any other entity, organization, or group that is incorporated to do business in the United States. It also includes any governmental (Federal, state, or local) entity. It does not include any foreign person.

3.3 Foreign Person

Any natural person who is not a lawful permanent resident as defined by 8 U.S.C. 1101(a)(20) or who is not a protected individual as defined by 8 U.S.C. 1324b(a)(3). It also means any foreign corporation, business association, partnership, trust, society, or any other entity or group that is not incorporated or organized to do business in the United States, as well as international organizations, foreign governments, and any agency or subdivision of foreign governments (e.g., diplomatic missions).

3.4 Item(s)

Defined in 15 CFR 772.1. Items include commodities, software, and technology. Commodities include any article, material, or supply except technology and software. Software includes a collection of one or more programs or microprograms fixed in any tangible medium of expression. Technology includes information for the development, production, use, operation, installation, maintenance, repair, overhaul, or refurbishing of an item.

3.5 Exporting

The act of sending, taking, or releasing items which are tangible (e.g., commodities) or intangible (e.g., technical data, software), outside the United States or anywhere to a foreign person including inside the United States. Exporting includes shipment as well as oral, written, electronic, or visual disclosure. For example, encryption software source code or object code that crosses an international border. Exporting includes the release of any technology, technical data, source code, or service subject to export controls to any foreign person whether abroad or in the United States (termed a deemed export). Deemed exports may occur through such means as a demonstration, e-mail, computer access, oral exchanges, or visual inspection of equipment and facilities, as well as the electronic transmission of controlled information or technology. Such exchange is deemed to be an export to the foreign person's country.

3.6 United States Munitions List (USML)

A list of articles, services, and related technical data designated as defense articles and defense services. The State Department has stated that the USML is illustrative only, meaning that the absence of an item on the USML does not conclusively rule out the possibility of its being a defense article or defense service.

3.7 Defense Article

Defined in 22 CFR 120.31. It includes any item or technical data that is specifically designed, developed, configured, adapted, or modified for a controlled use listed on the USML. In addition to the items on the USML, models or other items that reveal technical data related to USML items are also considered to be defense articles. Defense articles do not include basic marketing information on function or purpose or general system descriptions.

3.8 Defense Service

Defined in 22 CFR 120.32. The definition includes: 1) furnishing of assistance, including training, to a foreign person, whether in the U.S. or abroad, in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of defense articles; 2) providing any

foreign person any technical data as defined above; and 3) military training of foreign units and forces, regular and irregular, including formal or informal instruction of foreign persons in the United States or abroad or by correspondence courses, technical, educational, or information publications and media of all kinds, training aid, orientation, training exercise, and military advice.

3.9 Technical Data

Defined in 22 CFR 120.33. Technical Data includes information required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles. This information includes blueprints, drawings, photographs, plans, instructions and documentation. ITAR technical data also includes classified information relating to defense articles and defense services, information covered by an invention secrecy order and software directly related to defense articles.

3.10 Software

Software includes the system functional design, logic flow, algorithms, application programs, operating systems, and support software for design, implementation, test, operation, diagnosis, and repair. Software includes computer programs (a set of instructions that direct a computer to perform a sequence of tasks), procedural design documents (material that describes the procedural steps involved in the creation of a computer program), program documents (material created for the purpose of aiding the use, maintenance, or other interaction with a computer program), and databases (a collection of data elements grouped together in an accessible format).

3.11 Public Domain

Defined in 22 CFR 120.34. Public domain information is information which is published and which is generally accessible or available to the public. The ITAR describes means by which public domain information might be available, which include:

(1) Through sales at newsstands and bookstores; (2) Through subscriptions which are available without restriction to any individual who desires to obtain or purchase the published information; (3) Through second class mailing privileges granted by the U.S. Government; (4) At libraries open to the public or from which the public can obtain documents; (5) Through patents available at any patent office; (6) Through unlimited distribution at a conference, meeting, seminar, trade show or exhibition, generally accessible to the public, in the United States; (7) Through public release (i.e., unlimited distribution) in any form after approval by the cognizant U.S. government department or agency; (8) Through fundamental research in science and engineering at accredited institutions of higher learning in the U.S. where the resulting information is ordinarily published and shared broadly in the scientific community. Fundamental research is defined to mean basic and applied research in science and engineering where the

resulting information is ordinarily published and shared broadly within the scientific community, as distinguished from research the results of which are restricted for proprietary reasons or specific U.S. Government access and dissemination controls. University research will not be considered fundamental research if:

(i) The University or its researchers accept other restrictions on publication of scientific and technical information resulting from the project or activity, or (ii) The research is funded by the U.S. Government and specific access and dissemination controls protecting information resulting from the research are applicable.

3.12 Controlled Unclassified Information (CUI)

Unclassified information requiring safeguarding and dissemination controls mandated by statute or policy. Examples of such information include Official Use Only (OUO), Export Controlled Information (ECI), Unclassified Controlled Nuclear Information (UCNI), unclassified Naval Nuclear Propulsion Information (U-NNPI), Unclassified Controlled Information (UCI), Sensitive Unclassified Information (SUI), Statistical Information (STAT), Health Information (HLTH), Protected Health Information (PHI), and protected Personally Identifiable Information (PII).

3.13 Export Controlled Information (ECI)

Includes information (which may include technology, technical data, assistance or software), the export (including, as applicable, transfer to foreign persons within the United States) of which is controlled under the EAR, the ITAR, 10 CFR Part 810, or by OFAC. ECI is information scientific or technical in nature (STI). ECI is broadly defined and intended to capture a wide variety of STI. ECI may be found in: statements of work, conference papers, conference presentations, journal articles, abstracts, drawings, fact sheets, reports, memos, manuals, data sets, dissertations, instructions, blueprints, specifications, test data, engineering analysis, software, scripts, intangible files, patent applications, proposals, photographs, audio files, videos, or the like.

3.14 Scientific and Technical Information (STI)

Includes information products deemed by the originator to be useful beyond the originating site (i.e., intended to be published or disseminated), in any format or medium, which contain findings and technological innovations resulting from research and development efforts and scientific and technological work of scientists, researchers, and engineers, whether employee, contractor, or financial assistance recipient. STI also conveys the results of demonstration and commercial application activities as well as experiments, observations, simulations, studies, and analyses. Scientific findings are communicated through various media – e.g., textual, multimedia, audiovisual, and digital – and are produced in a range of products such as technical reports,

scientific/technical conference papers and presentations, theses and dissertations, scientific and technical computer software, journal articles, workshop reports, program documents and matter, patents, publicly available scientific research datasets, or other forms of STI. STI may be classified, Unclassified Controlled Nuclear Information (UCNI), Controlled Unclassified Information (CUI), Export Controlled Information (ECI), or unclassified with no access restrictions such as Unclassified Unlimited Release (UUR).

3.15 Personally Identifiable Information (PII)

Includes any information that permits the identity of an individual to be directly or indirectly inferred, which if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. PII includes but is not limited to the following: a) any of the following stand-alone elements: Full Social Security Number (SSN), Driver's license or State ID number, Passport number, Visa number, Alien Registration Number, Fingerprints or other biometric identifiers, or b) Full name in combination with: Mother's maiden name, Date of birth, Last 4 digits of SSN, Citizenship or immigration status, Ethnic or religious affiliation.

3.16 Protected Health Information (PHI)

Includes information transmitted or maintained in any form or medium (electronic, paper, oral or other) that (i) is created or received by a Covered Entity or any Health Care Component of a Hybrid Entity, (ii) relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and (iii) is identifiable to an individual or there is a reasonable basis to believe can be used to identify an individual. PHI is protected by HIPAA and includes any individual health information created, collected or received by any health care component of the university for either treatment or research purposes. PHI specifically includes but is not limited to the following, any PII field in combination with the following medical modifiers: Diagnosis or ICD code, Treatment or CPT code, Provider name or number, DEA number, Physician name, Treatment date, Patient notes, Psychiatric notes, Patient photos, or Radiology images.

3.17 FERPA Data

Includes records, files, documents, and other materials that contain information directly related to a student as a part of the student's Education Record or Treatment Record, maintained by the university or by a party acting for the university. FERPA Data includes but is not limited to the following: Grades, Class lists, Student course schedules, Disciplinary records, Student financial records, Payroll records for student employees (e.g. work study, assistantships, resident assistants).

3.18 Level One Data

Includes CUI, ECI, PHI, and PII.

3.19 Activities

Exports from any country, purchasing, software distribution, software development, research collaborations, proprietary work for others, sharing product specifications, item transfers, item shipments, international handcarry of items, hiring a foreign person, hosting foreign visitors, working with research students who are foreign persons, release of information, presentations, speaking engagements, electronic communications, facility tours, and the like.

4. Highly Regulated Destinations, Organizations, or Individuals

The United States Government limits U.S. Persons, including research and educational institutions, from conducting business or carrying-out other activities with various foreign persons. Some of these limitations apply to entire countries or destinations, while others focus on specific organizations, entities, or individuals. University personnel must receive approval from the export control office before initiation of any aspect of a project, task, or activity when the destination, country, government, agency, organization, entity, or individual is identified as embargoed, sanctioned, prohibited, restricted, having a policy of denial, or on an entity list.

4.1 Embargoed, Sanctioned, or Prohibited Destinations

The applicable destination-based regulations can change frequently. The EAR identifies embargoed countries and foreign persons. OFAC identifies sanctioned countries and foreign persons. The ITAR identifies embargoed countries and foreign persons. DOE and NRC also identify countries and foreign persons that require licensing.

4.2 Exempt Activities related to Embargoed, Sanctioned, or Prohibited Destinations

Many university activities do not require approval from the export control office when interacting with foreign persons based on specific exceptions in the export control regulations. In general, this exemption includes non-scientific, non-technical, and non-engineering activities. Activities exempt from approval by the export control office include:

a. Teaching of registered classes in the academic catalog so long as the technical nature does not go beyond general scientific, mathematical or engineering principles commonly taught in schools, colleges and universities;

b. Non-science, non-technical, and non-engineering faculty carrying-out non-science, non-technical, and non-engineering research on-campus so long as: software is not being used by a foreign person, goods are not being transferred to a foreign person, and the research is intended to be published openly with broad distribution; and

c. Conference presentations and conference dialogue open to the public in a non-embargoed, non-sanctioned, and non-prohibited country without a particular substantial interaction when discussing only information that lawfully exists in the public domain.

5. Highly Regulated Items and Services

The AECA confers on the U.S. President the authority to control the export of defense articles and defense services. The U.S. Department of State, Directorate of Defense Trade Controls (DDTC), issues the ITAR to implement the AECA. University personnel must receive express written approval from the export control office before initiation of any aspect of an ITAR-controlled project, task, or activity.

5.1 Defense Articles and Defense Services

a. University personnel must receive approval from the export control office before initiation of any aspect of a project, task, or activity that is designed, developed, engineered, manufactured, produced, assembled, tested, repaired, maintained, modified, operated, processed, or configured for use with respect to a military, space, or intelligence application or purpose. For instance, a space application or purpose may pertain to spacecraft, satellites, virtual satellites, space vehicles, or the like.

b. Information or software that is directly related to an item on the USML is likely ITAR-controlled unless the information or software: a) is already lawfully in the public domain, b) is basic marketing information on function or purpose, or c) is a general system description. General scientific, mathematical or engineering principles commonly taught in schools, colleges and universities are not ITAR-controlled.

5.2 STI-related Proprietary Information or Non Disclosure Agreements (NDAs)

University personnel must receive approval from the export control office prior to sharing export-controlled information with a foreign person. Proprietary data that is scientific or technical in nature may be export controlled information. The existence of an NDA related to the data or the data not being available to the public may indicate that the data is proprietary. Accordingly, university personnel must receive approval from the export control office prior to sharing, with a foreign person, proprietary information that is scientific or technical in nature.

5.3 Funding Source

University personnel must receive approval from the export control office before initiation of any scientific or technical aspect of a project, task, or activity that is funded via a defense-related, space-related, intelligence-related, or for-profit-related source. Such funding sources include DOD, DOE/NNSA, NASA, and for-profit corporations.

6. Inventions, Discoveries, Transfers, and Licensing

Items developed, modified, shipped, or disseminated by university personnel present various regulatory demands which may require additional paperwork to lawfully carry-out a transaction.

6.1 Inventions and Discoveries

The Office of Technology Transfer (OTT) must notify the export control office of any tangible invention or discovery that was built, constructed, created, generated, or modified using university resources before initiation of a process to transfer the invention or discovery outside of the university. OTT must notify the export control office of any invention or discovery for which any type of patent application is to be filed before the patent application is filed.

6.2 Transfers and Licensing

University personnel must receive approval from the export control office prior to licensing or disseminating software to a foreign person. University personnel must receive express written approval from the export control office prior to transferring, shipping, licensing, disseminating, or releasing any tangible item or software to a foreign person when the destination, country, government, agency, organization, entity, or individual is identified as embargoed, sanctioned, prohibited, restricted, having a policy of denial, or on an entity list.

7. Disclosures and Identification of Activities and Items

University personnel must disclose and identify activities and items related to potential exports and potentially controlled information.

7.1 Conflicts of Interest and NDAs

Any conflict of interest or conflict of commitment must be on record with the Office of Institutional Compliance and Ethics before initiation of any aspect of a project, task, or activity when the project, task, or activity includes both a scientific, technical, or engineering component and a foreign nexus component related to the conflict of interest or conflict of commitment. OTT must receive approval from the export control office prior to agreeing to an NDA that

includes both a scientific, technical, or engineering component and a foreign nexus component. For example, the foreign nexus component includes an association with a foreign person.

7.2 Marking

University personnel must mark items, such as documents or electronic files, that include CUI, ECI, PHI, or PII. Typically, marking occurs in accordance with the U.S. Government's CUI Marking Handbook. University personnel must mark all STI including items lawfully in the public domain. For instance, a publicly available document may be marked "Unclassified Unlimited Release."

7.3 Physical Safeguards

University personnel must physically safeguard CUI, ECI, PHI, PII, and ITAR-controlled items. The purpose of physical safeguarding is to prevent these items from being accessible to unauthorized individuals. To meet the minimum standard, university personnel must implement at least one physical barrier of protection. For example, the physical barrier can include a locked door, locked drawer, or locked file cabinet, provided that only those individuals with a lawful use and purpose have accessibility to the items.

7.4 Electronic Safeguards

Level One Data includes CUI, ECI, PHI, and PII. See University Data Classification Standards. University personnel must meet Boise State University Minimum Security Standards for Level One Data, as outlined on OIT Website to store or transmit Level One Data. Standards include, but are not limited to, requirements on encryption, logging, monitoring, authentication, documentation and backups.

8. Recordkeeping, Maintenance, and Records Retention

Individual departmental units must keep all records related to export-controlled items and services for five years after the conclusion of the project, task, or activity. University personnel must provide their affiliated individual departmental unit with the records, whether originals, copies, or back-ups. Records must be stored in a manner which facilitates the ability to retrieve them for any purpose during the five-year period, especially during an internal, State, or U.S. Government audit, inquiry, or investigation.

8.1 Export Licenses, Authorizations, Filings, and Technology Control Plans

The export control office must maintain records for export licenses obtained from the Department of State, Department of Commerce, or OFAC. Export authorizations otherwise obtained or filings with the U.S. government, such as the filing of an Electronic Export

Information (EEI), must be maintained by the individual departmental units associated with the project, task, or activity. Individual departmental units must keep all records related to technology control plans for five years after the conclusion of the project, task, or activity.

8.2 Foreign Travel

Individual departmental units must keep all records related to foreign travel by university personnel for five years after the conclusion of the travel consistent with Travel Policy 6180 and Public Records Management Policy 1020. If a travel service provider is utilized, the individual departmental unit responsible for the travel, working with Procurement and Vendor Services, must keep all records of any activities related to the travel. Exempt from recordkeeping is personal travel unrelated to the university such as foreign travel by university personnel that is not funded via the university, is not funded via a foreign source, involves no university items which are exported even temporarily, and is unrelated to the function of the university personnel at the university.

While traveling individuals must adhere to the technology standards outlined in the Boise State Minimum Security for Foreign Travel, as found on OIT's website.

8.3 Tangible Transfers

Individual departmental units must keep all records related to the transfer of a tangible item to a foreign person. The transfer of a tangible item to a foreign person includes hand-delivered transfers, international shipments, and the like. If a logistics service provider is utilized, the individual departmental unit responsible for the transaction, working with Procurement and Vendor Services, must keep all records of any activities related to the transaction. If filing of an Electronic Export Information (EEI) is required for any transfer, a logistics service provider must be utilized and all individual departmental units associated with the transaction must keep a copy of the filed EEI.

8.4 Software Dissemination

Individual departmental units, working with OIT, must keep all records related to software disseminated to a foreign person. Software dissemination records must include the export control classification for the software disseminated to the foreign person. The Minimum Security for Foreign Travel, as found on the OIT web page must be followed.

8.5 Release of STI

Individual departmental units must keep all records related to STI that is released for five years after the information is released. Individual departmental units may choose to require that all STI that is publicly released is to be published to ScholarWorks to streamline recordkeeping.

8.6 Foreign Visit Logging

Records of invited foreign person guests of university personnel must be kept by individual departmental units for invited foreign person guests who visit the university or access university resources. Individual departmental units, working with Human Resources, must keep all records related to citizenship and permanent residency for foreign persons receiving remuneration via the university. Remuneration includes a salary, stipend, honorarium, fringe benefit, tuition assistance, travel support, research support, or the like. Individual departmental units, working with Public Safety, must keep all records related to citizenship and permanent residency for foreign persons without remuneration via the university.

9. Related Information

Level One Data definition in Glossary of University Policy Terms
https://www.boisestate.edu/policy/glossary-of-university-policy-definitions/

Export Controls
https://www.boisestate.edu/research-compliance/export-controls/

U.S. Government's CUI Marking Handbook
http://archives.gov/files/cui/documents/20161206-cui-marking-handbook-v1-1-20190524.pdf

IT Standards
https://boisestate.edu/OIT-itgrc/it-standards-category/

Last Review Date