



Bureau of Industry and Security Compliance Note:

Trends in Voluntary Self-Disclosures Related to Academia to Inform Improvements to Export Compliance Plans

The Bureau of Industry and Security is dedicated to partnering with U.S. academic research institutions, both to protect national security and to help maintain U.S. leadership in innovation and collaboration. On June 28, 2022, Export Enforcement established the Academic Outreach Initiative to help academic institutions protect themselves from overseas threats and protect the security of their research. As part of this initiative, Export Enforcement has strongly encouraged Voluntary Self-Disclosures (VSDs) from academic institutions that believe that they may have violated the Export Administration Regulations (EAR).

To better support academia's compliance efforts, Export Enforcement provides the following observations on the nature and type of conduct amounting to violations of the export control laws that have been disclosed by academic institutions over the past ten years.

Biohazards

- **Conduct:** At least a dozen self-disclosures involved the unauthorized export of chemicals, microorganisms, and toxins, including vials or small quantities of biological agents such as Dengue-2 virus; and pathogens such as pseudorabies virus strains, genetically modified vesicular stomatitis virus, and isolates of *Magnaporthe oryzae*.
- **Analysis:** Much of this conduct occurred due to a lack of knowledge about the specific requirements for exporting small samples or vials of hazardous biological materials. Confusion over the classification of these items under the Commerce Control List (Part 774 of the EAR) (CCL) and misunderstanding of the export control requirements often contributed to these violations.
- **Remedial Actions:** Institutions have implemented more rigorous training programs for researchers and administrative staff on export control regulations, including clear guidelines on handling and exporting biohazardous materials. Universities have also enacted organizational changes, such as establishing new offices and working groups to administer export compliance programs as well as increased export compliance staff and resources. Additionally, enhanced tracking and documentation processes have been established to ensure compliance with EAR requirements.

Entity List

- **Conduct:** At least nine self-disclosures involved the unauthorized export of items to a party listed on the Entity List. Some of the transactions involved genetic material and genetically modified organisms, while one transaction involved the element hafnium, which is commonly used in nuclear reactor control rods.

- **Analysis:** This conduct often stemmed from a lack of awareness or confusion regarding the Entity List and the specific restrictions placed on listed organizations. Incorrect screening procedures, such as not screening all parties to a transaction (i.e., purchaser, intermediate consignee, ultimate consignee, and end user) and not re-screening transaction parties prior to shipment of items (e.g., only screening upon receipt of purchase order but not rescreening prior to shipment when it is possible that the Consolidated Screening List (CSL) has been updated in the interim) also resulted in export transactions with persons named on the Entity List.
- **Remedial Actions:** Universities have taken steps to improve their screening processes for international collaborations and shipments (both tangible and intangible), such as regular updates to their internal restricted party screening lists, requiring screening against the CSL at every step in the procurement process, including at time of export, and more thorough vetting of all parties to a transaction. Institutions also began using additional export compliance software to improve screening.

Deemed Exports

- **Conduct:** At least nine self-disclosures involved the unauthorized release of EAR-controlled technology to foreign national employees or students. These instances included technology related to electronics, telecommunications and information systems, and aerospace and propulsion. Four of the cases involved releasing EAR-controlled technology to Iranian nationals.
- **Analysis:** Conduct in this category was frequently due to universities' misunderstanding of deemed export rules and the requirement to obtain proper authorization before sharing controlled technology with foreign nationals. A lack of effective internal controls and training on export compliance also played a role.
- **Remedial Actions:** Universities have implemented mandatory training programs for staff and students involved in research and development. They have also established internal control systems to track and monitor the access of foreign nationals to controlled technologies.

Temporary Imports, Exports, Reexports, and Transfers (In-Country) (TMP)

- **Conduct:** Two self-disclosures involved exports improperly using license exception TMP, including one that involved infrared cameras that were hand-carried and exported from the United States. Among other things, TMP allows for the temporary export and reexport of various items subject to the EAR, as long as the items are returned no later than one year after export, reexport, or transfer if not consumed or destroyed during the period of authorized use.
- **Analysis:** The primary issue in these cases was the improper use of license exception TMP, often due to misunderstandings about the conditions and limitations associated with this exception. For example, universities have failed to submit a license application for an extension beyond the one-year limit of the TMP license exception.
- **Remedial Actions:** Institutions have clarified and reinforced the guidelines for using TMP license exceptions, ensuring that staff and researchers understand the specific conditions and limitations. They have also improved tracking mechanisms for items exported under this license exception to ensure proper usage and compliance.

Electronic Export Information (EEI)

- **Conduct:** Six self-disclosures involved academic institutions that failed to file EEI in the Automated Export System (AES) and undervalued items related to the export transaction.
- **Analysis:** Failures in filing EEI often resulted from insufficient knowledge about the regulatory requirements and the technical process for using AES. The absence of detailed export control procedures and training specific to the universities' operational needs also led to incorrect EEI documentation.
- **Remedial Actions:** Universities have provided additional training on the AES filing requirements and established more robust internal review procedures to ensure accurate valuation and reporting of exported items.

Recordkeeping

- **Conduct:** Three self-disclosures involved academic institutions that failed to maintain accurate export records. Universities have failed to maintain export records for the required five years, and in other cases, export records were either incomplete or non-existent.
- **Analysis:** Inadequate recordkeeping practices were generally due to insufficient training on export regulations and the importance of maintaining comprehensive and accurate records. Universities often lacked robust systems for tracking and documenting export transactions.
- **Remedial Actions:** Institutions have implemented better recordkeeping practices, including the adoption of electronic recordkeeping systems to track export transactions and regular internal audits to ensure reporting accuracy. They have also provided training to ensure staff understand the importance of maintaining detailed and accurate export records.

Information about the Bureau of Industry and Security's VSD policy can be found in Section 764.5 of the EAR, on the Export Enforcement [website](#), or by contacting the Office of Export Enforcement (OEE) at (202) 482-5036. Disclosures can be submitted electronically to BIS_VSD_INTAKE@bis.doc.gov. Furthermore, any person (i.e., not just a party submitting a VSD) may notify OEE that a violation has occurred and request permission from the Office of Exporter Services to engage in otherwise prohibited activities. These disclosures can be made through our [confidential reporting form](#). You can also call the Enforcement Hotline at 1-800-424-2980 or email EELead@bis.doc.gov.