Internal Guidance relating to DOJ Data Security Programs

Effective August 8, 2025

Background

On April 8, 2025, the U.S. Department of Justice (DOJ) launched the Data Security Program (DSP) under Executive Order 14117 to safeguard national security. The program restricts the transfer of sensitive personal and government-related data to certain foreign countries and individuals.

The DSP is designed to protect Americans' most sensitive data—including genomic, biometric, health, financial, and location information—particularly in transactions where the recipient did not collect the data directly.

Impact on Stevens (Faculty, Students and Staff)

Effective immediately, Stevens Institute of Technology has committed to compliance with the DSP by prohibiting all covered bulk transfers of sensitive data.

All members of the Stevens community must understand:

- What types of data are collected or stored about U.S. persons or devices.
- How that data is used, shared, or marketed.
- Whether any transactions involve covered data types, transactions or person.

Bulk Transfer Thresholds

Bulk data transfers are measured over a rolling 12-month period with the same parties. This means that repeated sharing over time can add up and trigger compliance requirements.

The term "sensitive personal data" means covered personal identifiers, precise geolocation data, biometric identifiers, human 'omic data, personal health data, personal financial data, or any combination thereof.

A transfer is considered "bulk" if it exceeds any of the following thresholds:

- 100,000 U.S. persons for personal identifiers
- 10,000 U.S. persons for financial or health data
- 1,000 U.S. persons for precise geolocation, biometric identifiers, or human 'omic data
- 100 U.S. persons for human genomic data

Note: These rules apply even if the data is de-identified, anonymized, pseudonymized, or encrypted. Such protections do not exempt the data from DSP restrictions.

Violations may result in significant institutional and personal consequences, including financial penalties and criminal liability.

Designated Countries of Concern & Covered Transactions

The DSP applies to U.S. entities engaged in transactions that could result in access to sensitive data by designated Countries of Concern or a Covered Person—defined as any individual or entity with ties to a designated country, such as being based in, controlled by, or acting on behalf of that country. This includes, but is not limited to: University employees, including faculty, staff, and administrators; contractors, consultants, and vendors engaged by the University; students and student employees; visiting researchers, scholars, or collaborators; and any other individuals acting on behalf of or at the direction of the University.

A transaction is considered covered if it:

- Involves a recipient from a designated Country of Concern or a Covered Person.
- Falls within a Covered Transaction Type.
- Includes a Covered Data Type.

Countries of Concern	Covered Transaction Types	Covered Data Types
China (& Hong Kong, Macau) Cuba Iran North Korea Russia Venezuela	Data brokerage Vendor agreements Employment agreements IT/cloud/network access arrangements	Bulk U.S. sensitive personal data U.S. government data

Required Actions

Your participation is essential to Stevens' compliance. Every member of the university community shares responsibility for protecting sensitive data and preventing prohibited transactions.

Please take the following actions:

- **Do not initiate or authorize any transaction involving covered data as defined by the DOJ Data Security Program**.
    - Any sponsored projects or research collaborations related to this guidance require prior review and approval by the Office of Sponsored Programs at contracts@stevens.edu.
    - If you have questions about whether past or recent activity may have involved covered data, or if you believe such a transaction may have occurred, please promptly contact support@stevens.edu for guidance.
- **Know your data**: Understand what data you collect, use, store, or share in your role. Be aware of where the data moves and who has access to it.
- **Before sending data** to an outside service or platform, confirm that it is not operated by or affiliated with a Covered Person.
- **Review data sharing** with any individual or entity potentially linked to Countries of Concern. When collaborating with foreign entities outside of designated Countries of Concern, ensure agreements include language prohibiting onward transfers to Covered Persons or Countries of Concern.
- **Ensure proper authorization** for contractors, vendors, and new hires. Contact support@stevens.edu to verify proper authorization before granting access to any data (e.g., encryption, role-based access, monitoring).
- **Monitor access**: Know who has access to data particularly when entering into contracts or agreements involving sending or receiving data and ensure compliance with the DOJ DSP.
- **Seek guidance:** If unsure whether a transaction is covered, contact support@stevens.edu.
- **Educate your team:** Ensure all team members understand and follow this guidance.

Additional Resources

For additional resources and information, the National Security Division (NSD) has published a Compliance Guide, an initial list of Frequently Asked Questions (FAQs), and an Implementation and Enforcement Policy.