ASCE

ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

International Travel Security:

Considerations When Implementing JCORE Recommended Practices and NSPM-33 Requirements

29 April 2022

Jessa Albertson, Stanford University

Scot Allen, Colorado School of Mines

Patrick Briscoe, University of Minnesota

Kelly Hochstetler, University of Virginia

Laura Provencher, University of Arizona

INTRODUCTION

This paper provides a risk-based approach to implementing international travel security recommendations and expectations put forth by the federal Joint Committee on the Research Environment (JCORE) and the National Science and Technology Council's related National Security Presidential Memorandum (NSPM-33) Implementation Guidance.

This overview is not exhaustive. The goal is to spark discussion and offer a range of potential measures for diverse universities with diversified research portfolios, resources, and risk tolerances.

BACKGROUND

International travel presents unique challenges and introduces risks requiring planning and oversight. Many universities employ a variety of practices and measures to evaluate and manage those risks. Existing programs typically evolved to meet a variety of needs: providing appropriate duty-of-care to international travelers; enabling fiduciary control; and facilitating compliance with federal regulations. Secure traveler programs also protect the security and integrity of university research.

Embedding research security practices into a comprehensive international travel program supports researchers, minimizes redundancy and confusion, and streamlines processes. Travel security practices protect people along with university initiatives, equipment, materials, and information.

SCOPE

To determine the appropriate scope for international travel security policies and procedures, universities can consider the following inherent risks:

DETERMINE SCOPE	**Travelers** • Faculty & staff only • Students • All	DESTINATION • High-risk countries only • All international destinations	**Activities** • Conferences • Lab research • Fieldwork • Lecturing • All purposes	**Funding** • Federal • Non-U.S. support • External non-federal support • Internal • Personal
EVALUATE RISKS	• International experience • Expertise • Institutional responsibility • Degree of oversight	• Regulatory (export controls/ sanctions) • Data/device security • Personnel safety & security • Host country laws	• Organizations involved • Traveler safety & security • Equipment and data	• Conflict of interest • Conflict of commitment • Contractual duties and liabilities • Federal requirements (Fly America Act, e.g.)

Universities should periodically evaluate each factor to appropriately tier pre-travel registration, review, guidance, and approval processes according to identified risks. Also consider implementation for international campuses.

STAKEHOLDERS

Effective oversight of international travel safety and security requires the coordinated efforts of a working group with cross-campus representation. Suggested representation includes:

FACULTY **LEADERSHIP** **FINANCE** **INTERNATIONAL OFFICE** **EXPORT CONTROLS** **IT SECURITY** **RISK MANAGEMENT** **STUDENT AFFAIRS**

Diverse stakeholder engagement facilitates a robust and efficient examination of risks and needs while maximizing insights on constituent perspectives and travel trends.

SPECIFIC MEASURES

Three primary categories of travel security measures align with the NSPM-33 Implementation Guidance:

Registration

Registration, planning, and screening

Technology security

Compliance and security awareness

Each category can be addressed with a range of measure and approaches.

INTERNATIONAL TRAVEL REGISTRATION, PLANNING, AND SCREENING

Universities may require pre-travel registration with elements tailored to address identified risks. Trip details determine which university offices or stakeholders should be consulted prior to departure.

Predeparture Registration Approaches

Least risk mitigation with lightest administrative burden:
Registration serves as documented notification to prompt guidance. No university *approvals* needed.

Targeted risk mitigation with moderate administrative burden:

Required registration prompts screening/assessment, guidance, and/or approvals from specialized offices and/or unit supervision for trips meeting defined risk criteria, such as—

- Travelers involved in **restricted or classified research**.
- Travel to comprehensively **sanctioned countries**.
- **Increased health, safety, and security risks** in destinations determined by State Department Travel Advisories, CDC travel health notices, etc.
- Involvement of **Parties of Concern** on the Commerce Department's Entity List, the Treasury Department's Sectoral Sanctions List, other federal and sponsored lists requiring special export or financial restrictions, or lists published by credible public sources of organizations presenting risks to research security or institutional values. (There is no single, objective list or set of risk criteria; universities should develop particularized standards, consistent with their own assessments of the material export, security, contracting, IP, and funding considerations.)
- **Funding from certain federal or other external sources**.
- **Providing services requiring federal approvals** to a foreign person or country.
- **Transporting or transferring controlled equipment, samples, materials, or data.**
- **Security briefing** in defined circumstances (see Compliance & Security Training below).

Greatest risk mitigation with heaviest administrative burden:

University assessments and approvals for the above criteria required prior to departure for *all* international trips.

Recommended Registration Information

TRAVELER	Involvement in export-controlled, classified, or other restricted research **Emergency Contact Information** to provide security alerts, emergency support, and other assistance.
FUNDING	To identify conflicts of interest/commitment and other regulatory or ethical risks.
DESTINATION(S) & DATES	To tailor review, screening, guidance, and approval processes, particularly regarding: ○ Sanctions and embargoes. ○ IT security compromise. ○ Health, safety, and security risks.
ACTIVITIES	Involved entities, to identify high-risk entities through restricted party screenings.

TECHNOLOGY SECURITY

Many universities have data security guidelines and requirements, including appropriate measures to identify and protect sensitive information.

Technology Security Guidance

AWARENESS

Enhancing cybersecurity awareness of the need to identify, protect, detect, respond, and recover (***as described in JCORE recommendation 21***) should be a part of the international travel registration process.

Cyber-hygiene guidance may be distributed by email or posted online and may include information regarding:

- **IT security resources**
- **Tips for safeguarding** personal devices and information
- **Minimizing social media** posts prior to and during travel
- **Not leaving devices unattended**, particularly in publicly accessible areas
- **Avoiding the use of public, unsecured internet** connections
- **Using only trusted, university approved flash drives** or other removeable media
- **Not installing new software** while abroad
- **Changing passwords** on return to the U.S.
- **Scanning** university and personal devices for malware upon return.
- **“Wiping” or reimaging devices**

Note: When feasible, universities should notify prospective travelers when destinations restrict the use of certain encryption, VPN, or other security measures.

DATA DISCIPLINE

Advise travelers to minimize data transported or accessed while abroad.

Particularly identify and safeguard data subject to regulations and laws, which include—

- International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EAR)
- Controlled Unclassified Information (CUI)
- Personally identifiable Information (PII)
- Protected health information (HIPPA)
- Student information (FERPA)
- Sensitive financial information

Protecting sensitive data with encryption and/or limiting storage and access on U.S.-based university servers via virtual private network (VPN) or other secure connection. Access to restricted data must be managed in accordance with export controls and information security requirements.

SANITIZED DEVICE OPTIONS	
Advise travelers to only transport necessary devices. **Provide** sanitized "loaner" electronic devices to reduce the risk of data loss or theft due to confiscation, device compromise, data replication, and local government scrutiny.	
LEAST RISK MITIGATION	Offering and encouraging, but not requiring: ○ general use of loaner devices. ○ loaner devices in units engaging in export-controlled or other high-risk activities.
TARGETED RISK MITIGATION	Require only high-risk travelers (e.g., cleared personnel and/or researchers working on export-controlled projects) and individuals traveling to high-risk destinations to use loaner devices.
GREATEST RISK MITIGATION	Require all international travelers use loaner devices.
The resources required to establish and maintain loaner programs can be significant, depending on the volume of travel, unique needs of research travelers, range of devices offered, software updates, and replacement of equipment. Personnel and space will also be required for, customized set-up, check-in/out, storage, wiping, and reimaging devices after travel.	

COMPLIANCE & SECURITY AWARENESS

Travelers should receive compliance and security guidance tailored, as feasible, to specific activities, destinations, and traveler vulnerabilities (JCORE recommendation 19.E). Such guidance may be provided online or during live pre-travel briefings.

Compliance & Security Topics	○ **Compliance requirements**—reminding travelers of U.S. export controls and sanctions. ○ **Awareness** of one's surroundings to identify, avoid, and deter potential threats to personal or information security. (Keeping in mind limitations even with local familiarity.) ○ **Threat indicators**—potentially compromising conditions, including crime, detention, government corruption, and intelligence activities. ○ **Criminal activity and political and economic instability** in destination(s). ○ **Local laws and cultural expectations**. ○ **Import/customs, tax, visa/immigration, and other legal requirements** of the destination.

Post-travel debriefings, whether in person or electronically (by email or survey) provide the opportunity to obtain additional information about potential concerns or requirements, such as reporting gifts, receiving suspicious offers, potential security or regulatory issues, or other unusual occurrences, as indicated in JCORE recommendations 13.A-G and 15.

CONCLUSION

Universities need comprehensive approaches to managing international travel that enhance travelers' health, safety, and security while protecting research and university resources and interests. Peer institution policies, processes, and lessons learned can provide valuable insights to facilitating an intuitive, streamlined, and fruitful registration process with user buy-in and increased compliance.

GOVERNMENT RESOURCES

- Centers for Disease Control: International Travel, COVID-19 Travel Recommendations by Destination
- Department of State: Travel Advisories, High-Risk Area Travelers, Safety and Security Messaging
- Federal Bureau of Investigation: Safety and Security for the Business Professional Traveling Abroad, Business Travel Tips, Safety and Security for US Students Traveling Abroad
- Office of the Director for National Intelligence: Traveling Overseas with Mobile Phones, Laptops, PDAs, and Other Electronic Devices, Safe Travels, Travel Awareness Video

Acknowledgement

The Academic Security and Counter Exploitation (ASCE) Working Group that developed this product was established to tap the expertise of universities with demonstrated excellence in academic security and counterintelligence programs. These programs intend address threats of espionage and inappropriate exfiltration from U.S. academic institutions.

The group includes representatives from a variety of universities, from those that conduct fundamental research only to those that conduct classified research on behalf of the federal government.

You can receive additional information about the Academic Security and Counter Exploitation Program and request membership information by emailing ASCEP@tamus.edu.