NSF SECURE Center

TRAVEL RESOURCE GUIDE

Last updated: 02/17/2026
Version 1.0.2

TABLE OF CONTENTS

CONTENT OVERVIEW 3
TRAVEL CHECKLISTS 4
INSTITUTIONAL CONSIDERATIONS 5
- GIFT ACCEPTANCE 6
- VISA CONCERNS 7
- PROTECTIONS FOR U.S. NATIONALS 7
- HEALTH & SAFETY 8
- CUSTOMS & CULTURAL CONSIDERATIONS 8
- LOANER DEVICE PROGRAMS 9
- EXPORT CONTROLS 10
- RED FLAG INTERACTIONS TO REPORT 11

CASE STUDIES 13
RESOURCES 14
APPENDIX 15

NSF SECURE Center

This material is based upon work supported by the U.S. National Science Foundation under Cooperative Agreement No. 2403771.

The NSF SECURE Center is intended for general research and educational purposes only. While we strive to ensure the accuracy and reliability of our content, we do not guarantee its completeness, timeliness, or applicability to specific circumstances. Each user is responsible for conducting their own risk assessments and making decisions based on independent judgment. Further, the NSF SECURE Center, including its website, does not provide professional or legal advice, and users are encouraged to consult qualified professionals before making decisions based on the information found here. The NSF SECURE Center and other U.S. government agencies shall not be liable for any damages or costs of any type arising out of or in any way connected with your use of the NSF SECURE Center, its services, or its information. External links are provided for convenience and do not constitute an endorsement of the content or services offered by any third-party resources.

CONTENT OVERVIEW

The Travel Resource Guide is designed to help faculty, researchers, and staff protect institutional resources, including intellectual property, data, unpublished research results, and personal information while traveling. It provides travelers with guidance on how to secure their digital footprint to address privacy and security concerns during travel.

The Resource Guide has been developed by the NSF SECURE Center and it is intended for Research Security Officers (RSOs) and/or other research administration professionals to share with faculty, researchers, and staff prior to travel.

TRAVEL CHECKLISTS

Basic Travel Checklist

The Basic Travel Checklist is designed to be used by all international travelers, from faculty to staff and those in the humanities and other basic science fields.
The checklist focuses on cybersecurity and other considerations for protecting research data, intellectual property, and personal information.

Travelers should use this product because it:

- Provides readers with clear, easy to understand information that can be applied in many different scenarios
- Allows for consistency and quality control for travel

FCOC & CET Travel Checklist

The FCOC Travel Checklist is meant to be used as a tool for travelers to high-risk foreign countries of concern or travelers that work on Critical and Emerging Technologies (CET).

Travelers should use this product because it provides additional steps and mitigation strategies for protecting data.

RESOURCE GUIDE

The Resource Guide gives additional context for the content on the checklist.

The travel case studies and resources included in this guide will give travelers a better understanding of the current travel risk landscape and some useful tips to prepare for travel.

The Resource Guide provides implementation considerations for rolling out a travel awareness campaign, as well as additional considerations about:

- Personal health & safety
- Visa requirements
- Cultural context
- Export controls
- Gift acceptance
- Institutional guidance on disclosures and other situations

TRAVEL BRIEFING

The briefing provides a structured curriculum for research security professionals to cover with travelers prior to departure. This resource is customizable and includes guidance on when and where to customize content.

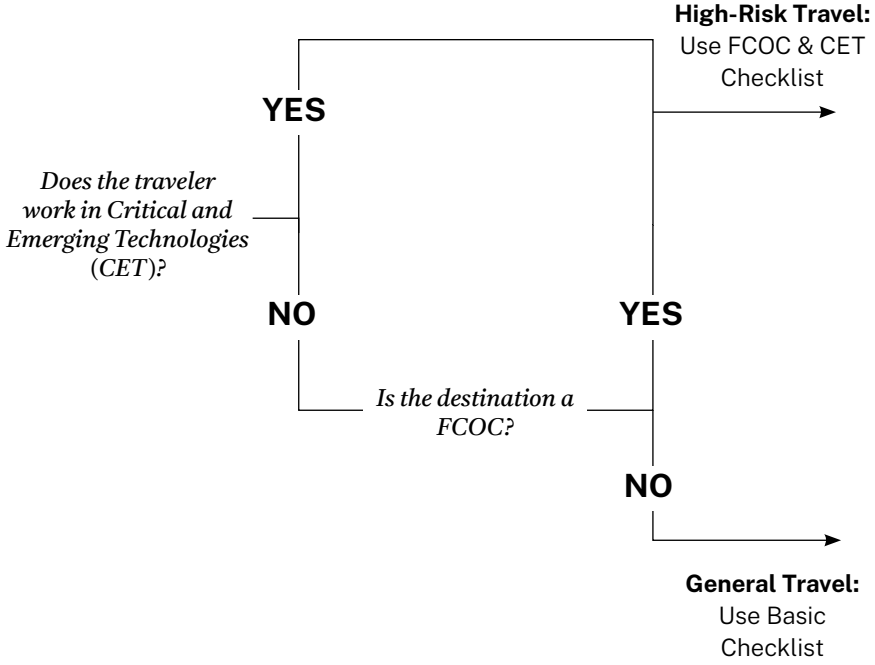
The Travel Briefing is geared towards travelers going to a FCOC and/or travelers working with CETs, and it has a high focus on cybersecurity best practices, with touch points on export controls and personal safety.

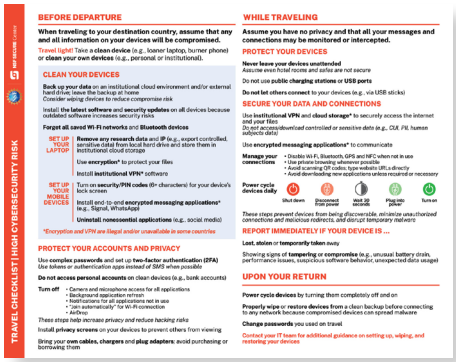
TRAVEL CHECKLISTS

Travelers, especially those with international itineraries need to be aware of the associated risks posed to the institution and the individual traveler. Risks can include cybersecurity and physical security concerns. These checklists can serve as a standalone resource or be utilized during a travel briefing. They are meant to serve as guidance, not rules.

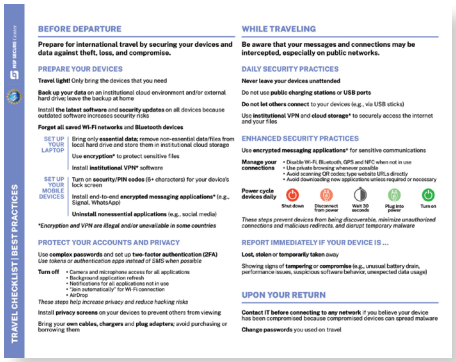
CHECKLIST TYPES

Both checklists provide guidance for travelers using their institution-provided and/or personal devices (i.e., laptops, phones, tablets), though the High-Risk Travel Checklist does mention that travelers should confirm if they need to take a loaner device.





Suitable for those traveling to FCOC and/or working in CET.



Suitable for the entire academic community, and for all travel. General best practices, focused on cybersecurity.

INSTITUTIONAL CONSIDERATIONS

Below is an overview of some common areas that institutions may need to provide additional guidance in order to ensure that travelers understand their obligations. These areas have not been included in this iteration of the checklists because the obligations may be very situation-specific and/or based on institution type.

- Personal health & safety
- Visa requirements
- Cultural context
- Export controls
- Gift acceptance
- Institutional guidance on disclosures and other situations

GIFT ACCEPTANCE

Travelers on professional travel must be cautious about accepting gifts from foreign sources due to various ethical and legal considerations. Institutions should provide clear guidance around gift acceptance while abroad. FAQS should help faculty and staff familiarize themselves with relevant university policies, applicable government regulations (like the FGDA), and ethical guidelines regarding foreign gifts to avoid potential conflicts of interest, legal issues, or the appearance of impropriety.

Here are some key points to keep in mind:

FOREIGN INFLUENCE AND CONFLICTS OF INTEREST

Accepting significant gifts from foreign entities could create the appearance of a conflict of interest or even lead to unwanted foreign influence on research or institutional matters.

It's important to ensure relationships with international collaborators are based on lawful, efficient, and fair practices, not influenced by personal gain.

Institutions should establish clear guidance on when and how to report any gifts received during travel.

LEGAL REPORTING REQUIREMENTS

Public institutions and government employees may have additional, state-specific reporting obligations. It is advisable that travelers are provided with clear guidance on their reporting obligations.

Institutions are required to report all foreign gifts and contracts from foreign sources exceeding a certain value (e.g., $250,000 or more annually), per Section 117 of the Higher Education Act (20 U.S.C. § 1011f).

SPECIFIC GIFT LIMITATIONS (FEDERAL EMPLOYEES)

In some cases, specific regulations like the Foreign Gifts and Decorations Act (FGDA) may limit the value of gifts that can be accepted from foreign governments or international organizations by federal employees.

For example, under 5 U.S.C. 7342, a federal employee may not accept a gift exceeding $480 in value from a foreign government or an international organization.

In some cases, faculty with joint appointments at a VA or a national laboratory may need to be mindful of these additional rules.

INSTITUTIONAL POLICIES

Universities, hospitals, and research institutions have their own policies regarding gift acceptance. These policies typically outline review and approval processes for gifts, especially those of significant value and/or from foreign sources.

EXPORT CONTROL REGULATIONS

If the gift involves hardware, software, or other materials, export control regulations may apply. This could necessitate obtaining an import license.

VISA CONCERNS

There are several visa options for faculty and staff, such as J-1, H-1B, E-3 (Australian citizens), O-1 (extraordinary ability), and TN (Canadian and Mexican citizens) visas.

WHEN ENTERING THE U.S., TRAVELERS WILL NEED THE FOLLOWING:

Required Documents

All travelers must have a valid passport, a valid visa (or be visa-exempt), and their specific visa document (e.g., DS-2019 for J-1, I-797 for H-1B).

DS-2019 Travel Signature

J-1 scholars must obtain a travel signature on their DS-2019 form from their program sponsor before traveling outside the US to ensure smooth re-entry.

I-94 Record

Upon entry, a CBP officer creates an electronic I-94 record, which serves as proof of lawful entry and status.

WHEN LEAVING THE U.S., TRAVELERS MUST REMEMBER THE FOLLOWING:

For travel less than 30 Days

J-1 scholars can generally travel outside the U.S. for personal or business reasons for less than 30 days.

H-1B visa holders can also travel abroad, but it's important to carry documentation demonstrating continued employment, even for short trips.

For absences Longer Than 30 Days

J-1 professors and research scholars can be absent for more than 30 days if doing research work outside the U.S.

Automatic Visa Revalidation

In some cases, H-1B visa holders may be able to re-enter the U.S. from Canada or Mexico without a new visa stamp if their travel is less than 30 days and they meet certain requirements.

Travelers with visas may have additional requirements based on institutional policies.

PROTECTIONS FOR U.S. NATIONALS

Travelers going abroad may wish to review the Department of State "Consular Protection of U.S. Nationals Abroad". For those traveling to high-risk countries, the best protections are checking with the Department of State on travel advisories, enrolling in the Smart Traveler Enrollment Program, maintaining low profiles, and carefully considering personal security in making travel choices.

Those needing help abroad can contact the U.S. Embassy. Any citizen may call 1 202-501-4444 from outside the United States to contact the local Embassy. We recommend that travelers consider having a business card with the local number of the US Embassy, as well as the number listed here.

The U.S. has signed agreements with several countries to offer specific protections to visiting scientists; any harassment should be reported immediately to the Consulate or the U.S. Embassy.

HEALTH & SAFETY

Travelers should keep the following in mind when planning international travel:

HEALTH CHECKS & IMMUNIZATIONS
Check destination-specific health information and consult healthcare providers regarding required or recommended immunizations and medications

HEALTH INSURANCE
Ensure adequate health insurance coverage for the trip, including medical evacuation and repatriation

STAYING HEALTHY
Be aware of common traveler's illnesses like foodborne, waterborne, or airborne infections and take precautions to minimize risk

MEDICAL EMERGENCIES
Know how to handle health emergencies abroad and have contact information for emergency services and relevant university offices

PERSONAL SAFETY
Be aware of any safety alerts posted on the State Department or other traveler's websites

CUSTOMS & CULTURAL CONSIDERATIONS

When traveling abroad, it's essential to be aware of local customs and etiquette to ensure respectful interactions. Here are some key points to consider:

GREETINGS
Learn basic greetings in the local language and adapt your approach based on the culture. For example, in Japan, a bow is customary, while in many Western countries, a firm handshake is the norm.

DRESS CODES
Dress appropriately for the local culture. In some countries, revealing or suggestive clothing may be seen as disrespectful. For instance, in Saudi Arabia or Iran, women are expected to cover their heads and wear loose-fitting clothing.

LANGUAGE AND GESTURES
Use clear, polite language and gestures. Simple gestures like a thumbs-up or the "OK" sign might seem harmless, but in Greece or Brazil, they can be offensive.

EYE CONTACT
Eye contact can vary in meaning. In the U.S. and Europe, maintaining eye contact is seen as a sign of confidence, while in Japan or South Korea, too much eye contact can be considered confrontational.

PERSONAL SPACE
Be mindful of personal boundaries and practice appropriate body language. In some countries, such as Japan or Finland, people highly value their personal space, and invading it can be considered rude.

LOANER DEVICE PROGRAMS

The checklists are geared towards institutions without loaner device programs. Institutions without loaner device programs will rely heavily on travelers to follow best practices related to cybersecurity while traveling internationally. RSOs should work with the IT department on institutional specific guidance to "clean" institutional/personal devices pre-travel to countries deemed high-risk.

For institutions with loaner device programs some additional areas of concern that may want to be discussed with travelers include, but are not limited to the following:

"CLEAN" DEVICES: LAPTOPS, PHONES, TABLETS

- Ensure travelers understand what options they have available for loaner devices
  - Clarify what devices the institution provides and which the traveler may still need to clean (i.e., the institution may provide a laptop but not a cell phone)
  - Does the traveler know where to pick up and return the device?
  - What is the process for requesting a loaner device?
- If a loaner device program does not exist or is not available for the person traveling, does the institution have specific guidance for cleaning devices before travel that differ from this guidance? Which should travelers adhere to?
- Emergency contact information: who should the traveler contact if they are not able to access VPN?

ACCESSING UNIVERSITY APPROVED CLOUD STORAGE ENVIRONMENTS

- Document available institutional guidance on the use of cloud storage during travel.
- Document the point of contact for travelers with questions about accessing a cloud environment during their travel.
- Document specific processes faculty need to follow for the ability to access data internationally, deliniating between low-risk countries and high-risk/FCOC where access may be blocked or restricted, such as Russia or Iran.

ACCESSING UNIVERSITY VPN

- Travelers should always use VPN while traveling, even domestically.
  - In some countries off-the-shelf VPNs are restricted (i.e., China, UAE). In such cases, the traveler should use the institution's VPN service for both personal and professional communications.
- Using a VPN helps protect travelers from geofencing, which is when apps or websites use your location to restrict what you can access based on where you are.

EXPORT CONTROLS

Below are some additional questions/areas of concern RSOs should consider when preparing international research travelers international travel:

- What items are travelers planning to take with them out of the US?
  - Could the item(s) qualify as a temporary export?
- What items are the travelers planning to bring back to the US?
- Are they shipping items to/from their destination? Is an export or import license required?
- Are there any specific customs requirements or export/import license requirements for any of the items if yes to the questions above?
- Are the travelers aware of what a deemed export violation is and how to avoid it, especially for those working in critical or emerging technology or export controlled technology?

RED FLAG INTERACTIONS TO REPORT

Below is an overview of some common areas that institutions may need to provide additional guidance in order to ensure that travelers understand their obligations. These areas have not been included in this iteration of the checklists because the obligations may be very situation-specific and/or based on institution type.

PHYSICAL INTERACTIONS

RSOs should advise travelers to be wary/proceed with caution with these scenarios:

- Do not enter any verbal/written agreements without first contacting the RSO at the institution.
- Acceptance of social media requests (i.e., LinkedIn) requests from individuals the traveler does not know.
- Careful consideration of any research related advice given/questions answered during lab tours. Providing guidance on highly technical export-controlled (i.e., military aircraft) or CETs could create a deemed export violation by the traveler. Travelers should be wary of providing any technical support.
- Invitation to attend a closed-door meeting or one in which no devices, cellphones and/or laptops are allowed.
- Ellicitation attempts to get the traveler to divulge information about unpublished research or the work of their colleagues.
- Request to carry items (materials, packages, samples) in or out of a country - this is never acceptable.
- Unusual surveillance, signs of physical intrusion or tampering of a traveler's personal belongings.
- Being separated from devices. Examples: a border agent taking the traveler's device for inspection or theft of one or more devices while traveling.

What are elicitation techniques?

- Subtle questioning
- Professional requests
- Exploiting expertise
- Flattery

CYBER THREATS

Travelers should be advised to report immediately to the institution's IT team if they believe their device has been compromised. These are some signs that a device may have been tampered with:

BATTERY AND PERFORMANCE ISSUES

Rapid battery drain and overheating, sluggish performance, and frequent freezing or crashing; these can be caused by unauthorized software running in the background.

UNUSUAL DATA USAGE AND APPS

Unexpected spikes in data usage or the appearance of unfamiliar apps can point to malicious activity.

SUSPICIOUS BROWSER BEHAVIOR

An increase in pop-up ads, changes to your browser settings, or new toolbars may indicate adware or malicious software.

ACCOUNT AND COMMUNICATION IRREGULARITIES

Unusual activity on online accounts, suspicious sounds during calls, or unsolicited requests for personal information.

UNEXPECTED DEVICE AND SECURITY SOFTWARE BEHAVIOR

Device is behaving unexpectedly, such as apps opening randomly, could mean that security software has been disabled.

UNAUHTORIZED CAMERA OR MICROPHONE ACTIVATION

Activity lights for webcam or microphone apps might turn on when they haven't been in use.

How to tell if a phone is being tapped?

Unusual sounds on calls
High-pitched hum, pulsating static, clicking, or beeping, could all be signs that your calls are being recorded

Your phone won't shut down or shuts down unexpectedly
Phone randomly turning off or rebooting may also be a sign of trouble

Websites don't look right
Some malware can infiltrate browsers by displaying fake web pages that look legitimate. Phishing scams like this are common because social engineering schemes work

Battery drains and phone overheats
This could mean there is malicious software that is constantly sending data back to whomever is tracking the phone. Go to settings and see which apps are running the battery down the most

CASE STUDIES

It is understandable that some travelers like to see evidence of travel concerns. The NSF SECURE Center hopes to build a repository of reported incidents. These are incidents reported in the media or by federal agencies:

RESEARCHER CHARGED WITH SMUGGLING FROG

Link to the article

Russian researcher Kseniia Petrova was returning from France where she collected frog embryo samples for her lab, when U.S. Customs at Boston Logan Airport detained her after discovering the undeclared biological materials in her luggage.

FOREIGN STUDENT CHARGED WITH SMUGGLING ROUNDWORM INTO THE US

Link to the article

Chengxuan Han, a Ph.D. student from Wuhan, China, was arrested at Detroit Metro Airport and charged with smuggling biological materials (specifically roundworm-related substances) into the U.S. and making false statements to federal agents. She initially denied sending any packages and falsely described their contents, and notably, had wiped her phone by deleting its data three days before arriving.

HOTELS NEAR BEIJING OLYMPICS GROUNDS REQUIRED TO MONITOR GUESTS' INTERNET ACTIVITY THROUGH INSTALLED SOFTWARE

Link to the article

During the 2008 Beijing Olympics, the Chinese Ministry of Public Security ordered hotels to install special software to surveil guests' internet usage. Failure to comply would result in fines, suspended access, or even business license revocation. The mandate (later confirmed by major international hotel chains) caused significant concern among hotel operators.

The NSF SECURE Center is continuing to look for case studies, if you have an example, it will be de-identified and you will be allowed to review any text before the case is posted. Please share your examples by emailing SECURENE@northeastern.edu

RESOURCES

"Alien from Wuhan, China, Charged with Making False Statements and Smuggling Biological Materials into the U.S. for Her Work at a University of Michigan Laboratory." *Department of Justice*, 9 June 2025, https://www.justice.gov/usao-edmi/pr/alien-wuhan-china-charged-making-false-statements-and-smuggling-biological-materials

Bencie, Luke. "Everyday Business Travelers Are Easy Targets for Espionage." *Harvard Business Review,* 10 November 2015, https://hbr.org/2015/11/everyday-business-travelers-are-easy-targets-for-espionage?cm_mmc=email-_-newsletter-_-management_tip-_-tip_date&referral=00203&utm_source=newsletter_management_tip&utm_medium=email&utm_campaign=tip_date

"Chinese government forces hotels to install internet spying tools." *Catholic News Agency*, https://www.catholicnewsagency.com/news/13387/chinese-government-forces-hotels-to-install-internet-spying-tools

"Export Controls: Temporary Exports | DoResearch." *DoResearch*, 29 May 2025, https://doresearch.stanford.edu/resources/topics/export-controls-temporary-exports

Government of Canada. "Remaining cyber safe while travelling: security recommendations - Travel.gc.ca." *Travel and Tourism*, 26 November 2024, https://travel.gc.ca/travelling/health-safety/cyber-safe/recommendations

Gundling, Katherine, et al. "A faculty-informed framework for responsible and equitable academic travel." *ScienceDirect*, September 2023, https://www.sciencedirect.com/science/article/pii/S2667278223000512

Harvard Global Support Services. "International Travel and Electronic Device Searches | *Harvard GSS.*" Harvard GSS, 2025, https://www.globalsupport.harvard.edu/travel/advice/international-travel-electronic-device-searches

"Harvard researcher charged with smuggling frog embryos is being released from federal custody." *CNN*, 12 June 2025, https://www.cnn.com/2025/06/12/us/harvard-researcher-frog-embryos-released

Mosaica. (2024). *The Cultural Atlas.* https://culturalatlas.sbs.com.au/

National Counterintelligence and Security Center. "Companies Travel Security Guidance Introduction." *DNI.gov*, 25 October 2024, https://www.dni.gov/files/NCSC/documents/SecureInnovation/10252024_Final_Travel-Security-Guidance.pdf

The National Counterintelligence and Security Center. "Travel Tips." *DNI.gov*, https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-know-the-risk-raise-your-shield/ncsc-travel-tips.

National Intellectual Property Rights Coordination Center. *Reporting Allegations of Intellectual Property Theft*. 2025. *National Intellectual Property Rights Coordination Center* (*IPR Center*), https://www.ice.gov/doclib/iprcenter/pdf/reporting_allegations_of_intellectual_property_theft.pdf.

"Potential 'agroterrorism weapon' fungus smuggled into US by Chinese scientists, FBI alleges." *The Guardian*, 4 June 2025, https://www.theguardian.com/us-news/2025/jun/04/potential-agroterrorism-weapon-fungus-smuggled-into-us-by-chinese-scientists-fbi-alleges.

Stanford University. "Export Controls: Temporary Exports." *DoResearch*, https://doresearch.stanford.edu/resources/topics/export-controls-temporary-exports.

Travel State Gov. "Travel Advisories." *Travel State Gov,* https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html/

US Department of Justice. *Safety and Security for the Business Professional Traveling Abroad. FBI*, https://www.fbi.gov/file-repository/counterintelligence/business-travel-brochure.pdf/view.

APPENDIX

The following appendix provides supplementary guidance on:

- Institutional implementation
- Multiple appointments
- Travel briefings
- Roles

INSTITUTIONAL IMPLEMENTATION

Each institution will vary in how it approaches international travel. At some institutions, the checklists could be embedded in a travel registry and emailed to all travelers, but at other institutions, automation may be impractical or out of step with the institutional culture.

Broadly speaking, institutional implementation should consider the following questions:

- Who are the stakeholders that need to be involved?
  - Who would be responsible for communicating and enforcing any research security travel considerations?
  - Does the institution currently brief faculty on international travel?
  - See the roles section below for some ideas.
  - Does the institution have a travel registry or another process for vetting, approval and tracking of travel? Does this system apply to the whole community or just a specific subset?
- Is the registration and approval process automated?
- Can or should travel guidance be disseminated via automated messages?
- Does the institution have travel policies?
- Where will institutional travel resources be housed? Will this information be public or private?
- Does your institution have or is considering a loaner device program?
- Where should faculty report any travel incidents? What will the institution do when they receive the reports?
- What kind of records will the institution maintain related to travel guidance and advisories, as well as reported travel incidents?
  - Many institutions offer additional travel insurance for free or low cost when registering travel. Understanding what the institution offers for travel insurance may help in promoting the value of travel registration and may be woven into communication about your institution's travel resource guide.
- What is the plan for developing faculty and staff awareness of travel guidance?
- Communication planning is critical for success. Institutions should consider:
- Will a senior leader communicate the rollout of any tools and guidance?
- Who is the institution targeting in communicating these resources?
- Are these mandatory or recommended practices?
- Who will do outreach and what might that outreach look like to various stakeholder groups?
- Do you have any CET labs or other groups on campus that need additional and personalized communications?

Working with the stakeholders you identify, it is possible to develop your program by running through tabletop exercises and identifying where you need to scaffold additional policies, procedures and resources with gaps you identify.

The SECURE center has developed some tools to help facilitate that journey here.

MULTIPLE APPOINTMENTS

Some faculty may have dual appointments at multiple institutions. An example of this might be a faculty member with an appointment at both a university and its accompanying medical center or a faculty member at a university that also has an appointment at an independent research institute.

Each institution will have its own policies and procedures that require multi-appointment individuals to remember multiple standards. Institutions may wish to coordinate with other organizations to understand what guidance is provided to travelers that have multiple appointments, especially with respect to:

- Training obligations and records
- Travel registration and briefings
- Dissemination of tools and resources for travel (including checklists)
- The use of loaner devices
- Reporting concerns or incidents that occurred during travel

Understanding where faculty may have diverging or competing obligations to multiple institutions can help with coaching faculty as they navigate the complexities of multiple appointments.

TRAVEL BRIEFINGS

Institutions may wish to do individualized outreach to all or some faculty preparing for international travel, either based on destination location and/or research area (i.e., CET and/or controlled/sensitive research).

Personalized travel briefings may not be realistic for all international travelers. Understanding general travel patterns, research portfolio, and institutional risk tolerance are important to consider when determining which travelers should receive a travel briefing and which may receive written guidance and/or generic training. Institutions may wish to consider the following curriculum for briefings:

- How is research security relevant in the context of travel
- Some generic risks associated with research security and travel
- Relevant country specific considerations
- Additional context for any recommendations on the checklist that would be especially important for the traveler to follow based on destination and research area

ROLES

These will vary by institution, but these are some recommended ways to think about who should engage when implementing the tool kit at your institution. We use the RACI methodology in our documents.

ROLES	TITLE
Responsible	RSO Research Compliance Officer
Accountable	IT Global Safety Team or Travel Team
Consulted	Vice President for Research Office of General Counsel Faculty senate or other faculty body Export Control Officer
Informed	Research administrators Faculty Other administrators in the institution with a role in travel

NSF SECURE Center

https://www.secure-center.org