COMPANIES

National Counterintelligence and Security Center

SECURE INNOVATION

TRAVEL SECURITY GUIDANCE

INTRODUCTION

Emerging technology companies of all sizes are being targeted by certain nation states. Companies with weak security are most at risk. Adversarial countries may steal your technology to:

- Fast-track their technological capability, undermining your competitive edge
- Target, harm, and repress their own people to prevent dissent or political opposition, damaging your reputation
- Increase their military advantage over other countries, risking our national security

Travel to those countries, or third-party countries where hostile actors can operate without scrutiny, could put your people and innovation at risk. This guidance is designed to help companies develop a travel security policy to help overcome the primary counterintelligence and security challenges presented when working or traveling overseas.

THREATS

There are a range of ways in which security can be compromised in the course of foreign business travel. Awareness of these risks will help you introduce effective travel security policies to protect your staff and your business. Someone who wants to get access to emerging technologies will be looking to:

- Identify targets
- Access sensitive documents and information, electronically or physically
- Recruit insiders in target organizations

Think about how the following situations could highlight your company as a prospective target, put your IT and information at risk, or be the start of a recruitment or compromise attempt.

BEFORE TRAVEL

- Details provided on visa applications or customs declaration / immigration forms
- Details of travel plans shared on social media
- The information you share with your hosts

IN-TRANSIT

- Accessing devices at borders
- Charging points
- Public Wi-Fi
- Theft of unattended items

AT HOTELS

- Eavesdropping
- Internet connections
- Access to rooms or safes, during or after your visit

AT MEETINGS, CONFERENCES, SOCIAL EVENTS

- Internet connections
- Theft or copies of papers or devices
- Eavesdropping
- Probing questions
- Offers of expenses-paid trips
- Bluetooth-enabled conference tracking devices

WHEN YOU RETURN

- Attempts at further contact
- Suggestions of further paid overseas trips
- Phishing attempts

BEFORE YOU GO

UNDERSTAND THE RISKS

Ensure you understand the environment you are traveling to and any legal risks by considering the following:

- State Department notifications on travel to a country/countries
- Countries subject to U.S. sanctions
- The legal and legislative environment in the country you are traveling to
- Also think about the reason for your travel. Are you confident about the legitimacy and credibility of the people you will be meeting?
- Research your hosts to assess the risks of the visit

These considerations will help you make an informed decision about the benefits and risks of traveling overseas to achieve your business objectives.

KNOW YOUR "RED LINES"

Before travel, take time to consider the information you are comfortable sharing to achieve the objectives of the trip.

- Think carefully about what information you share or present.
- Be clear on the aspects of your business and innovation that you can, and cannot, talk about.
- Make sure all travelers are familiar with these red lines, and are empowered to be polite but firm if pressed to share more information.

LEGAL COMPLIANCE

There may be laws and regulations you will need to comply with in the country where you or your colleagues are traveling. Most countries will maintain some form of export control; they may have laws which restrict their organizations' ability to share data or project outcomes; and the legal protections around intellectual property (IP) may also differ in those jurisdictions.

Think about:

- Briefly researching the legal and legislative environment in the destination country so you can understand the potential legal risks to your staff and your innovation.
- Checking whether the work conducted overseas is subject to U.S. or local export controls. If so, apply for appropriate licenses.
- If relevant, familiarize yourself with the IP framework and enforcement processes in the destination country.

CAUTION

Before travel, consider completing a risk assessment. Take a proportionate approach which considers the country you are visiting and the reason for your visit. Keep this under review up to the point of departure, as well as during the trip, as the situation may change quickly.

- Make sure someone in the U.S. (ideally a manager) has the traveler's itinerary and establish check-in times throughout the trip.
- Ensure your employees know what to do and who to talk to if anything suspicious happens while they are overseas. This could range from a contact taking an excessive interest in your company's intellectual property, to a laptop with company data being stolen. A positive security culture in which employees feel supported to raise any concerns will help with this.
- U.S. citizens may not have the same legal or constitutional rights when visiting other countries as they do at home, and should be more alert and mindful of their surroundings and local customs.

CYBER SECURITY

When traveling overseas, you likely will need to take some sort of mobile IT device with you, such as a laptop, tablet and/or mobile phone. However, think carefully about the work and personal information they contain and what the impact would be if any of the devices were lost, stolen or cloned. As a baseline, have no expectation of privacy on your devices when traveling abroad.

- Consider removing unnecessary data and files from any devices you take with you, or taking a clean device with you that only contains the information essential to the trip.
- Make sure devices are password/passcode protected and use other security features, such as fingerprint recognition. Passwords/passcodes should be unique for each account and device.
- Many email and social media providers offer multi-step authentication (MSA). Turn this on for important accounts. This makes it harder for other people to access your accounts and can provide alerts if others are attempting to access your accounts without your permission.
- Make sure that all software and apps are up to date prior to leaving the U.S. If you are taking a laptop, make sure that your antivirus software is turned on, USB auto-run is turned off, the laptop is password protected and will not automatically connect to Wi-Fi networks.

- Make sure you know how your device will connect to both the internet and company systems when you reach your destination. If your organization uses a Virtual Private Network (VPN) or other security technology, ensure you know how it works and what to do if something goes wrong.
- Never download apps from unofficial providers, either in the U.S. or abroad. Unofficial app stores cannot be trusted; there is no way of knowing if the app is genuine.
- Consider activating device-wide encryption.
- Make sure phones can be wiped if they are lost or stolen.
- Back up all your data and photos before you travel.

DURING YOUR TRIP

The risks of international travel will vary depending on the nature of the travel. The steps taken before traveling will help manage the risks you or your colleagues are exposed to. However, there are risks you must be aware of during your trip.

IN-TRANSIT

Air travel and security checks at ports mean you will not have constant control over your electronic devices and luggage. There is a risk that someone could access your devices or assets while you are traveling.

- Traveling only with the information you are willing to share, both in physical and electronic formats, will reduce the risks of unintended exposure of your assets.

DURING YOUR STAY

- Check-in at the agreed points with a U.S.-based colleague. Make sure they are aware of any changes to your itinerary.
- Hostile actors could gain access to your hotel rooms, and capable actors can get into hotel safes. Hotel safes can be used for the storage of valuable items, but should not be used to store sensitive information.
- Be alert that a hostile actor could try to recruit your staff while they are traveling. Being approached in person or online before or after a meeting, or during a conference could be the start of a recruitment attempt. If a staff member experiences any suspicious approaches, they should let a U.S.-based colleague know as soon as possible.
- Public and hotel Wi-Fi connections may not be safe; carefully consider what information you might be sharing when using these connections. Avoid internet banking abroad and implement the guidance above for all other accounts.
- Consider the use of VPNs to manage communication back to the U.S. However, be aware of any local rules on VPN usage, which is normally permitted but access must be provided if requested by law enforcement.

WHEN YOU GET BACK

Being security conscious does not end when you leave the country you were visiting. You may recognize security issues when you return to the U.S.

- Let points of contact at your organization know that you have returned safely.
- Record any incidents that occurred while overseas.
- Let your company know if anyone has approached you since your trip - either in person or online.
- If anything indicates that your accounts or devices have been tampered with, reset passwords and supporting credentials, and report the incident to your company.
- Check your possessions for signs of tampering and report any issues with your electronic devices to those responsible for information security in your organization. Lessons learned from your experiences can be used to improve travel security procedures and support future travelers.