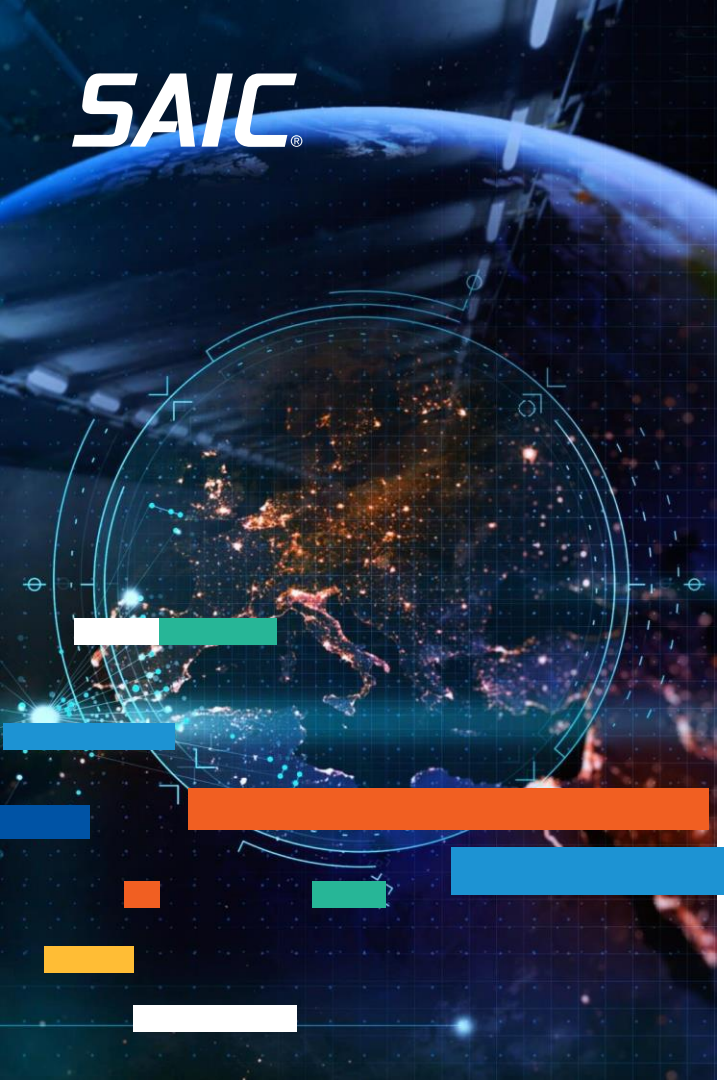


DEFENSIVE INTERNATIONAL TRAVEL BRIEFING

SAIC International Security Program

TABLE OF CONTENTS

TRAVEL PREPARATION

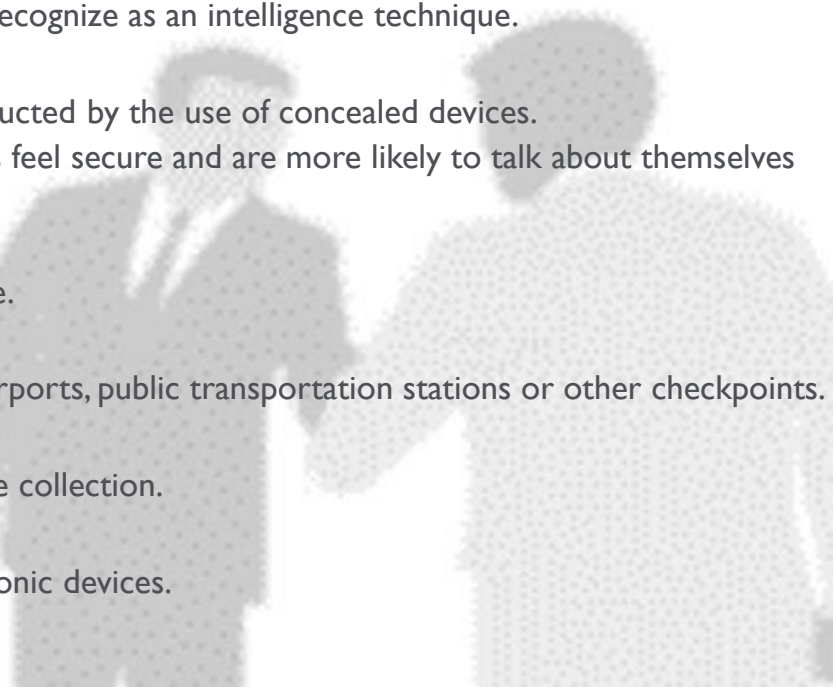
- **Before You Travel**
  - Employees must submit an International Travel Request (ITR) on ISSAIC prior to traveling overseas
    - Subcontractors/Consultants must submit a pre-travel form
    - Personal foreign travel reporting is a requirement for cleared employees, subcontractors and
    - consultants
    - Personal foreign travel reporting highly recommended for uncleared employees
  - Be aware of the local laws and customs
  - Make copies of your passport and other important documents
  - Register with the U.S. State Department's STEP Program, which allows U.S. citizens traveling abroad to enroll with the nearest U.S. embassy or consulate

INTERNATIONAL TRAVEL RISK OVERVIEW

- **Technology developed by the U.S. is targeted by foreign nations.**
  - It is less expensive to steal technology than it is to develop new technology
  - This threat pertains to both classified and unclassified information
- **Cleared defense contractors are vulnerable to Foreign Intelligence Entities (FIE) due to their access of sensitive or classified information**
- **FIE typically target sensitive or classified information, cutting edge technologies, or information critical to U.S. infrastructure. They may also target exploitable vulnerabilities in people.**
- **FIE will use a variety of collection methods in order to access information.**
- **Common sense and basic counter-intelligence awareness can protect you against FIE activities.**

INFORMATION COLLECTION METHODS

- **Elicitation**
  - A ploy where a seemingly normal conversation is contrived to extract information (FBI Elicitation Manual).
  - Puts someone at ease to share information and is difficult to recognize as an intelligence technique.
- **Eavesdropping**
  - Listening to conversations to gather information, may be conducted by the use of concealed devices.
  - Frequently conducted in social environments where attendees feel secure and are more likely to talk about themselves or their work (bars, restaurants and public transportation).
- **Direct Questioning**
  - Simple and direct questions that do not obscure their purpose.
- **Secondary Screening**
  - Additional questioning conducted by FIE usually at customs, airports, public transportation stations or other checkpoints.
- **Honey Trap**
  - Romantic blackmail or coercion for the purpose of intelligence collection.
- **Physical Searches**
  - Covert searches of hotel rooms, vehicles, belongings or electronic devices.

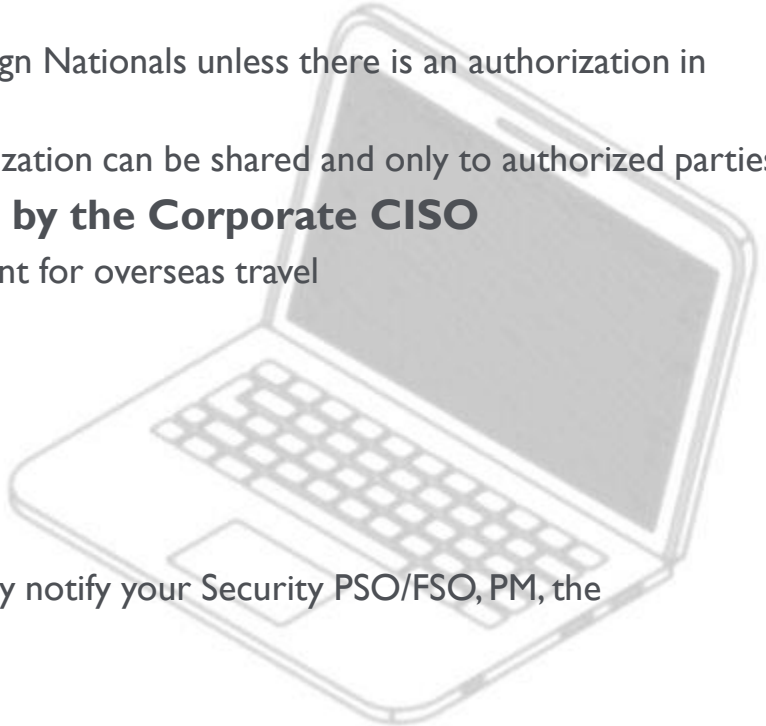


INFORMATION COLLECTION COUNTERMEASURES

- Change the topic of conversation
- Refer the questioner to publicly available resources
- Ignore or deflect inquiries or conversation, give vague answers
- Keep sensitive material until it can be properly disposed of
- Never check your computer with your luggage, always carry it with you
- Do not leave sensitive documents or equipment unattended in hotels (even in hotel safes)
- Do not discuss sensitive topics outside of approved spaces
- Do not use computers or fax machines at foreign hotels or business centers
- Do not let anyone borrow your electronic devices
- Be alert, be aware and always report suspicious occurrences to your **SAIC PSO/FSO** and the **SAIC Counterintelligence & Threat Mitigation Team**

ITAR / EAR & SAIC DEVICES

- **The International Trade and Compliance Office must provide approval for all exports in accordance with ITAR and EAR Regulations.**
  - Do not share any export-controlled information with Foreign Nationals unless there is an authorization in place.
  - Only technical data covered by an approved, current authorization can be shared and only to authorized parties
- **Taking SAIC devices overseas requires approval by the Corporate CISO**
  - In some circumstances, SAIC can issue employees a thin client for overseas travel
  - If approved to take an SAIC device overseas
    - Use your VPN
    - Avoid using Bluetooth
    - Only use your personally owned charger
    - You must always keep positive controls over all devices
    - If your SAIC device is lost or stolen, you must immediately notify your Security PSO/FSO, PM, the International Trade Office and ITO.



PERSONAL SECURITY

- **Remember, you are subject to the local laws of which you are traveling**
- **Remain alert and always maintain caution**
- **Only stay in reputable hotels**
- **Do not use the hotel phone to discuss travel plans**
- **Avoid public transportation**
- **If possible, travel in a group**
- **Have a working knowledge of the local language**
- **Maintain a low profile**
  - Blend in with your surroundings
  - Conceal material wealth
  - Exchange U.S. currency for local currency

EMERGENCY ASSISTANCE WHILE OVERSEAS

Even with the best preparations, things can go wrong.
Know where to seek assistance should an emergency occur.

- **International SOS can provide the following assistance to SAIC employees who are traveling overseas (employees on personal travel will pay out of pocket for extraction services).**
  - In country assistance for lost passports or assistance with currency exchanges
  - Direction to local hospitals or clinics for medical attention
  - Extraction from country in dire circumstances
  - U.S. Embassy location and contact information
  - Instruction on how to obtain police, fire or ambulance services while in-c
  - Country intelligence and threat level information

For More Information: www.internationalsos.com
Member # 11BYCA083835

THREAT AWARENESS VIDEO

[Know the Risk – Raise Your Shield: Travel Awareness Video]

Video produced by SAIC for the ODNI.

REPORTING PROCEDURES POST TRAVEL

- **When You Return**
  - Employees must complete the post-foreign travel questionnaire through ITRS on ISSAIC
  - Cleared subcontractors and consultants must complete the post-foreign travel from and submit to their SAIC PSO/FSO
  - Report any suspicious activity to:
    - Your local PSO/FSO
    - SAIC Counterintelligence & Threat Mitigation Team. (CITM@saic.com or via ES3)

HAVE A SAFE TRIP