DCSA Foreign Travel Briefing

Non-Specific Country

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Presented by First Last Name
Counterintelligence Special Agent
DCSA (Region) Region

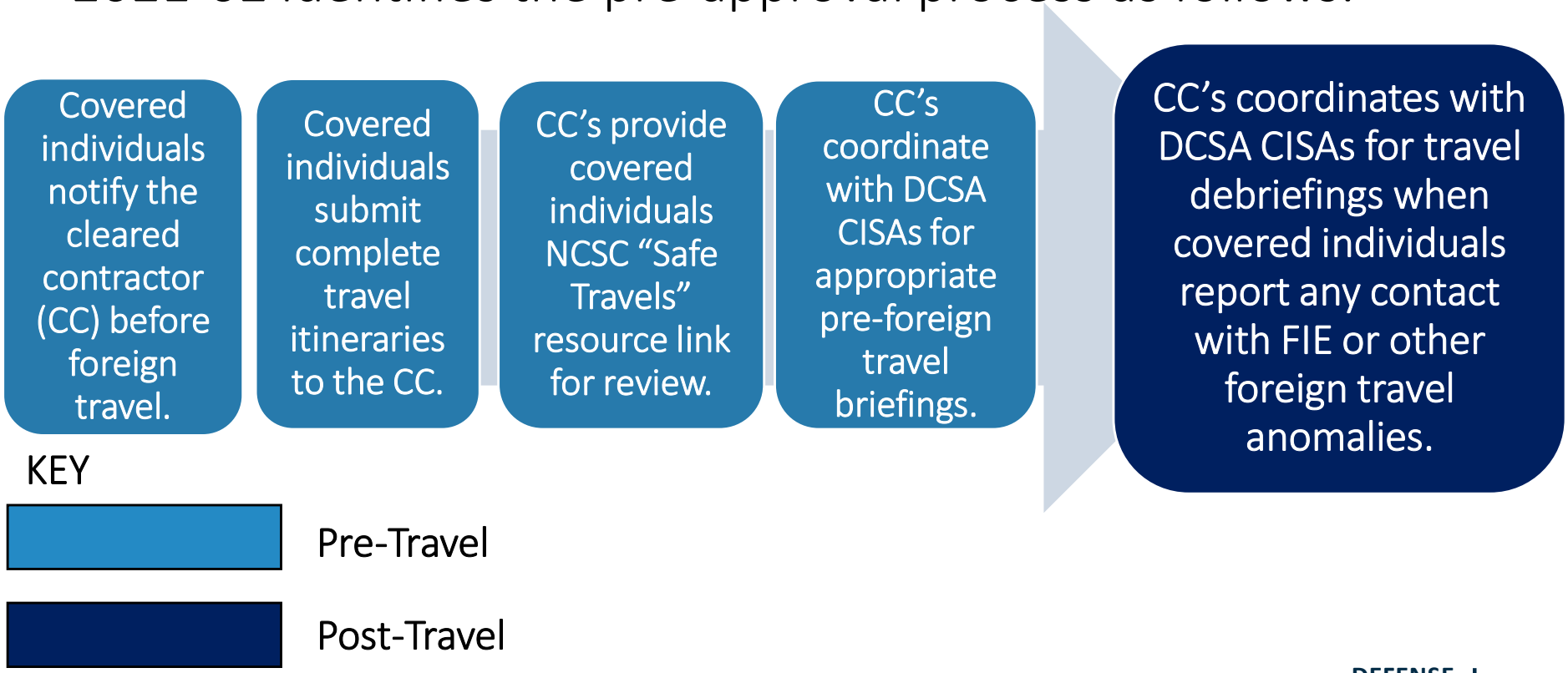
Agenda

- Introduction
- Foreign Intelligence Entities
- Vulnerability Awareness
- Elicitation and Countering Elicitation
- Personal Safety
- Information Security
- Terrorist Threat
- Before You Go
- When You Return

Introduction

Unofficial Foreign Travel Approval Process:

- Covered individuals under DoD National Industrial Security Program security cognizance are required to received approval prior to unofficial foreign travel. Industrial Security Letter (ISL) 2021-02 identifies the pre-approval process as follows:



Introduction

What is Unofficial Foreign Travel:

- Unofficial foreign travel: All travel other than that defined by "official foreign travel," and includes any foreign travel conducted before, during, or after official foreign travel, and that does not meet the criteria of "official foreign travel" as stipulated below
- Official foreign travel: Foreign travel by covered individuals that is in direct support of an established U.S. Government contract with the ultimate customer being the U.S. Government, whether as a prime contractor or a sub-contractor

Introduction

What is Counterintelligence (CI)?

- Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against:
  - Espionage,
  - Sabotage,
  - Other foreign intelligence activities
- Conducted by, for, or on behalf of:
  - Foreign Intelligence Entities
  - Foreign persons or their agents,
  - International terrorist organizations

- Against U.S. national security interests or DoD and its personnel, information, materiel, facilities, and activities

Foreign Intelligence Entities

Foreign Intelligence Entities (FIE):

- Known or suspected foreign groups or individuals, (public, private, or government) that conduct activities to acquire U.S. information, influence U.S. policy, or disrupts U.S. systems and programs

Economic Espionage:

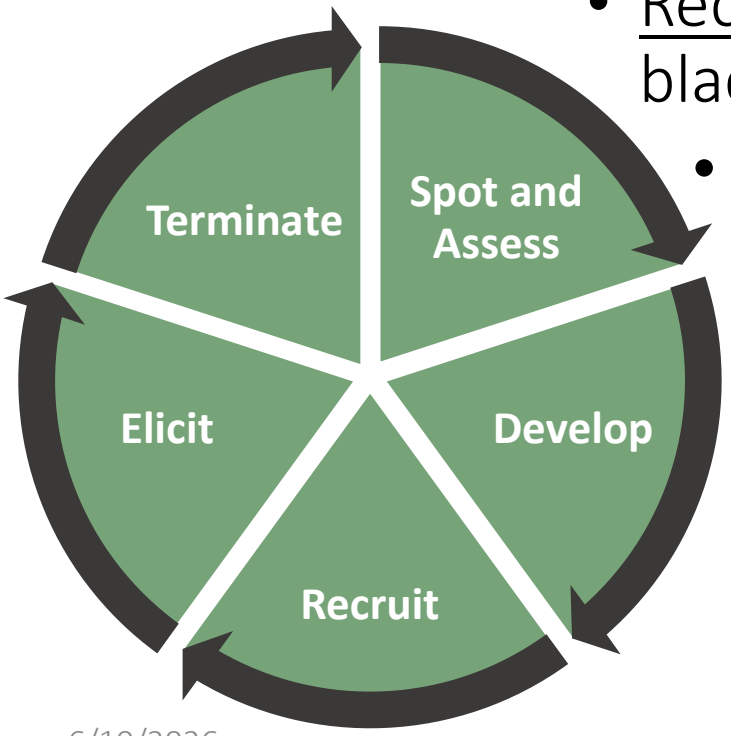
- FIE activity directed at U.S. corporations or persons, to unlawfully or clandestinely influence economic policy decisions or obtain sensitive proprietary information or critical technologies
- Provides FIE with proprietary information at a fraction of the cost of its research and development, causing significant economic loss

CI and Security awareness can help limit exposure to exploitation attempts by FIE during travel!

Foreign Intelligence Entities

How FIE operates:

- Spot and Assess: Identify someone who might have access to sensitive information or key personnel
- Develop: Initiate and build a relationship using similar interests or other motives
- Recruit: Appeal to ideology, financial gain, blackmail coercion, etc.
- Elicit: Exploit the target's access to information, wittingly or unwittingly
- Terminate: Conclude activities or end the relationship once the information or access is no longer valued



Vulnerability Awareness

Why is this briefing important to me?

- RISK of being targeted is greater while traveling abroad:
  - FIE have more opportunities to interact
  - FIE often operate in countries other than their own, including those that are friendly to the United States
- CI and Security awareness prior to travel can:
  - Help limit exposure to exploitation attempts by FIE and criminal elements during travel!
  - Bring awareness to serious safety and security concerns regarding travel to your destination

You are the first line of defense in protecting sensitive information and defense technologies!

Vulnerability Awareness

Why would I be a Target!

- FIE operate around the world to recruit and run paid agents in U.S. companies and government entities
- U.S. cleared industry is a prime target of FIE and foreign government economic competitors
- Cleared Contractors may have access to:
  - Classified or sensitive information
  - Emerging technologies and pioneering research
  - Information critical to infrastructure

Vulnerability Awareness

Be aware!

- Personal devices transmit information on foreign networks
- Travelers have reported searches of hotel rooms
- FIE have various means of screening incoming visitors and compromising electronics
- Targeting could include:
  - Elicitation: suspicious questioning or a pitch, (in-person or otherwise)
  - Surveillance: Physical or electronic monitoring
  - Coincidentally meeting someone who shares your interests or a “Honeypot” ruse

Vulnerability Awareness

FIE Collection Techniques.

- Physical:
  - Elicitation
  - Hotel room and safe intrusions
  - Enhanced interviews by customs officials
  - Surveillance: bugged hotel rooms or airline cabins
- Cyber:

- All electronical information, fax, computer, or phone, can be intercepted
- Wireless devices are especially vulnerable
- Activity can be tracked via ATM transactions and Internet usage
- Installation of malicious software in electronic devices at customs or in hotel

Elicitation

Elicitation:

- The strategic use of conversation to extract information without giving the feeling of being interrogated
- FIE and criminals are adept at pretending to be someone you can trust to obtain personal or sensitive information

Elicitation Methods:

- Feigned Disbelief
- Provocative Statement
- Questionnaires and Surveys
- Quote Reported Facts
- Ruse Interviews
- Volunteering Information / Quid Pro Quo, Etc.

Elicitation

Examples of FIE elicitation:

- Requests for protected information under the guise of a price quote, purchase request, market survey, etc.
- Attempts to entice personnel into situations that could lead to blackmail or extortion
- Attempts by foreign customers to gain access to hardware and information that exceeds the limitations of the export licenses on file
- Attempts to place personnel under obligation through special treatment, favors, gifts, or money

Prompt reporting is a mechanism to get necessary attention and support before the situation escalates!

Countering Elicitation

Elicitation is not rare, be prepared!

- Work in pairs, the most successful elicitation occurs when the target is alone!
- Be observant of people during engagements and suspicious of people seeking unauthorized information
- DO NOT provide unauthorized or personal information about family or colleagues
- Practice responses to potential questions
- You are NOT obligated to answer questions that make you feel uncomfortable
- Remain professional and non-committal, and avoid expressing opinions

Countering Elicitation

What can I do if approached!

- Change the subject or walk away if a conversation is too probing concerning your duties, private life, and co-workers
- Feign ignorance or change the subject
- Challenge the question: “Why do you ask?”
- Be direct: “I cannot discuss the matter”
- Deflect questions with one of your own
- Be boring by providing generalized answers

Report After Returning to the United States!
Do not discuss with colleagues!

Personal Safety

Local Laws:

- You are subject to local laws and FIE are not restricted by U.S. laws!
  - Violating local laws, even unknowingly, may result in expulsion, arrest, or imprisonment
  - Be aware of cultural expectations
  - DO NOT make assumptions about what is acceptable
  - DO NOT take photographs in the vicinity of foreign military bases, buildings, or personnel

Personal Safety

Crime:

- Crime is one of the biggest threats facing travelers
- Crimes against travelers are often crimes of opportunity
- Follow these steps to protect yourself:
  - Ensure hotel rooms have a peephole and a bolt lock, when possible
  - Stay alert
  - Be wary of street vendors and youngsters who may be decoys for pick pockets
  - Minimize the cash you carry
  - Exercise good judgment

Personal Safety

Arrest, and Detention:

- Foreign police and intelligence agencies can arrest and detain for many reasons, even curiosity
- If detained or arrested:
  - Stay Calm and professional
  - Request authorities immediately notify the U.S. Embassy or nearest Consulate
  - DO NOT provoke the arresting officer
  - DO NOT admit to anything or volunteer any information
  - DO NOT sign anything until the document is examined by an attorney or an embassy/consulate representative
  - DO NOT fall for the ruse of helping the ones who are detaining you in return for your release

Personal Safety

Hotel Safety Tips:

- Only patronize reputable hotels
- Note escape routes, secure doors
- Keep windows locked
- Keep your room key with you
- DO NOT accept unrequested deliveries
- DO NOT use the hotel phone to discuss travel plans
- DO NOT stay in hotel rooms that are located on the first floor or easily accessible from the outside

Be aware! Some countries require passports to be left with hotel reception over night, to be checked by local authorities!

Personal Safety

Travel Safety Tips:

- Be alert and cautious
- Travel in groups, whenever possible
- Carry a charged cell phone
- Keep your wallet in your front pocket avoid handbags
- If carrying a bag or backpack, zipper locks are recommended
- Learn the parts of town locals consider risky and avoid them
- AVOID isolated areas, civil disturbances, and large crowds
- AVOID using unmarked taxis
- DO NOT place valuables in the trunk
- DO NOT use taxis outside of the normal taxi stand/lane

Personal Safety

Maintain a Low Profile:

- New surroundings and exotic destinations may be distracting
- Do not reference your government related duties or access to sensitive information
- Do not publicize “post” travel plans
- Drive an inconspicuous vehicle
  - Vary where you park
  - Keep at least one-half tank of gasoline
  - Keep car windows closed
- Conceal material wealth, exchange money for local currency, and dress like the locals

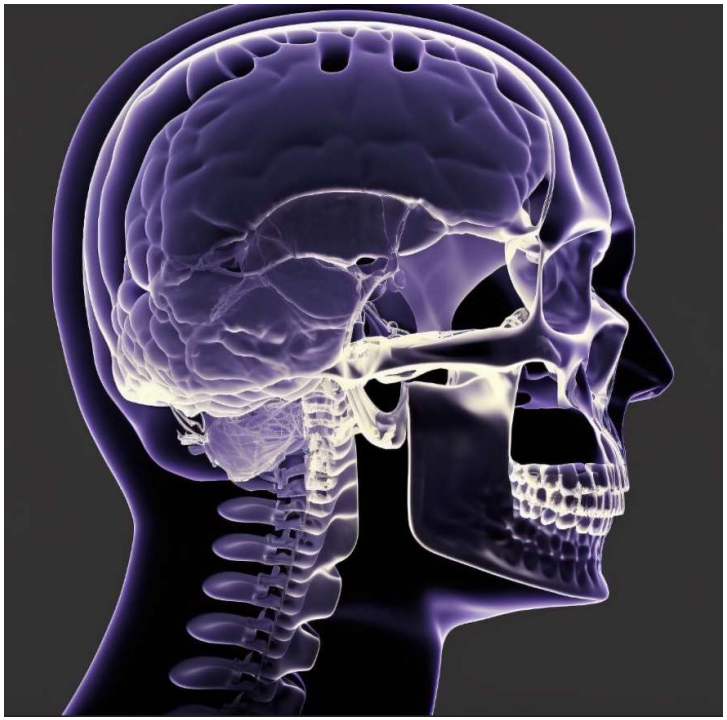
Personal Safety

Anomalous Health Incidents (AHI):

- Sudden onset of unexplained, unprompted events of sensations of sounds, vibrations, heat, or unexplained physical discomfort

Typical symptoms:

- Headache, pain, nausea, vertigo
- Sounds, pressure, and heat



What to do:

- Immediately remove yourself, coworkers and family members from the area (Get off the "X")
- Seek necessary medical attention
- As soon as possible, report suspected AHI to your chain of command, security officer, or the DCSA CI element

Information Security

Before Travel:

- DO NOT bring personal electronic devices you don't need!
- Fortify electronic devices and secure personal information:
  - Use strong passwords, (Long, Random, and Unique)
  - Update operating systems and security software
  - Use two-factor authentication for sensitive accounts
  - Delete sensitive information
- Disable the geo-tagging feature to protect personal information about your location

Information Security

During travel: (Be Vigilant!)

- Use lock screens and cover screens when entering passwords, pins, and accessing sensitive information
- Secure devices while in public places, e.g., airports, hotels, and restaurants
- Use a VPN while using public Wi-Fi at airports, hotels, etc.
- For sensitive transactions (e.g., banking or purchases) use “https://” or “shttp://” for secure communications
- Periodically disconnect from public Wi-Fi networks
- DO NOT make purchases or access financial accounts and other sensitive information on unsecure networks
- DO NOT use public USB charging stations

Information Security

During Travel:

- Only share personal information and security efforts with trusted friends and security personnel
- DO NOT download apps or connect to unknown devices

After Travel:

- Be cautious when responding to unsolicited text messages or voicemails
- Perform anti-virus and malware scans on all electronic devices
- Change all passwords

FIE can track your movements using your cell phone and can turn on the microphone even when you think it's off

Terrorist Threat

Be Aware:

- Extremists and criminals target U.S. citizens around the world and attack "soft" targets including:
  - Tourist locations, transportation hubs
  - Shopping malls and markets
  - Hotels, clubs, and restaurants
  - Places of worship, schools, parks
  - High-profile public events: sports, rallies, holiday events, etc.
- Avoid or do not spend too much time at “Soft” targets!
- Have a plan, know where to go during an incident

Find known local terrorist and criminal threats @ U.S. Department of State information: https://travel.state.gov/.

Terrorist Threat

Take Precautions:

- Schedule direct flights to avoid stops in high-risk airports
- Watch for abandoned packages or other suspicious items
- Monitor local media for breaking news, adjust plans as needed
- Blend in with your surroundings, i.e., dress like the locals
- Travel with others and carry a charged cell phone
- Avoid publicity and establishing routines
- Identify safe areas, e.g., police stations, hotels, and hospitals
- During a terrorist attack, leave the area if possible. If not, hide and as a last resort, yell and fight

Before You Go

Additional Resources:

- U.S. Department of State (DOS): Travel (state.gov)
  - Travel advisories, messages, and Alerts
  - Passport, VISAs, restrictions, vaccinations
  - Embassy contacts, website, and address
  - Smart Traveler Enrollment Program (STEP)
  - Health information and COVID restrictions
- Central Intelligence Agency (CIA): Countries - The World Factbook (cia.gov)
- Federal Trade Commission: FTC Online Privacy and Security
- Office of the Director of National Intelligence (ODNI): DNI SEAD3 Toolkit

Before You Go

Additional Resources:

- DCSA, Center for Development of Security Excellence (CDSE):
  - Counterintelligence (CI)
  - CI Awareness Toolkit
  - FSO Toolkit
  - Traveling with Mobile Devices
- DCSA, CI and Insider Threat Directorate
  - SEAD 3 Unofficial Foreign Travel Reporting
  - DCSA Reports, Flyers, Posters, and Handouts

When You Return

REPORT FOREIGN CONTACTS:

- Known or suspected FIE
- Bonds of affection, personal obligation, or intimate contact
- Suspicious interactions, activity or unexpected events
- Exchanges of personal information
- Significant changes in the nature of the contact
- Blackmail, coercion, or elicitation of classified/protected information

In the aftermath of several espionage cases, co-workers commented that they noticed unusual behavior, but did not know how to report!

When You Return

Report before the situation escalates:

- Unwillingness to comply with rules, regulations, or security requirements
- Alcohol, Drug abuse, Criminal conduct
- Misuse of U.S. Government property or information system
- Use of a foreign passport for travel
- Probing questions, harassment, or searches by locals or officials
- Gifts from suspected FIE or FIE associates
- Suspicious approaches by foreigners
- Suspicious emails, text, social media invitations, or phone calls
- Contact your security official for a foreign travel debriefing upon return.

Provide as much information as possible to your security point of contact after returning to the United States!

2026 FOREIGN TRAVEL & SEAD 3

CERTIFICATE OF COMPLETION

I certify that I have been provided and completed the following training classes in accordance with the National Industrial Security Program Operating Manual (NISPOM):

DCSA Foreign Travel & SEAD 3 Briefing

_____ , 2026

Print Name **Date**

_____

Signature

Please sign, scan and send this certificate to your FSO.
If you do not have access, please email this certificate to: chinna@indexsystemsinc.com