

UNCLASSIFIED

DCSA Foreign Travel Briefing

Non-Specific Country

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY



7/1/2025

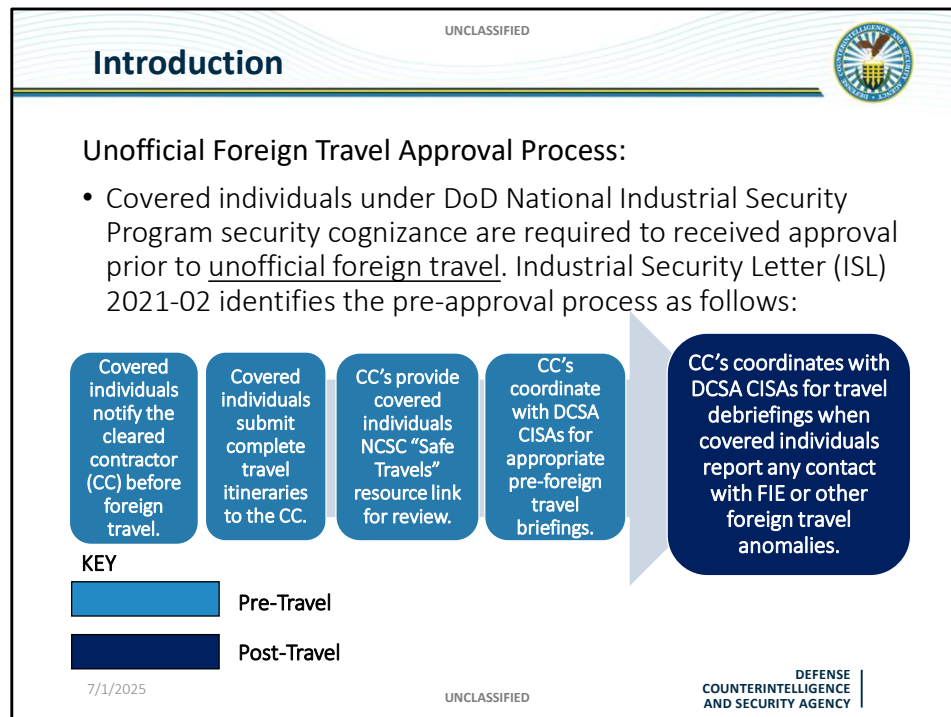
UNCLASSIFIED

DCSA-CI-24-010

Agenda



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



Additional Information:

1. Unanticipated border crossings into any foreign country not included in the traveler's approved itinerary, regardless of duration, are discouraged. All deviations from approved travel itineraries shall be reported within five business days of return.


Source(s):

DCSA Industrial Security Letter (ISL) 2021-02, 12 August 2021, Table 4, "Guidance and Clarification for NISPOM Rule Foreign Travel Reporting for all Covered Individuals".

Director of National Intelligence (DNI), Security Executive Agent Directive 3 (SEAD3), 12 June 2017, "Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position".


UNCLASSIFIED

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



UNCLASSIFIED

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY

7/1/2025

Additional Information:

SEAD3 Foreign travel reporting exemptions:

1. Travel to Puerto Rico, Guam, or other U.S. possessions and territories is not considered foreign travel and need not be reported.
2. Unplanned day trips to Canada or Mexico shall be reported upon return. Reporting shall be within five business days.
3. When required by the agency head or designee, covered individuals shall, prior to travel, receive a defensive security and counterintelligence briefing.
4. While emergency circumstances may preclude full compliance with pre-travel reporting requirements, the covered individual, at a minimum, shall verbally advise their supervisor/management chain of the emergency foreign travel with all pertinent specifics and, preferably, a security representative, prior to departure. In any event, full reporting shall be accomplished within five business days of return.

Source(s):

SEAD3, 12 June 2017, "Reporting Requirements for Personnel with Access to Classified Information or Who Hold a


Sensitive Position”.

DCSA ISL 2021-02, 12 August 2021, Table 4, “Guidance and Clarification for NISPOM Rule Foreign Travel Reporting for all Covered Individuals”.

Image: DCSA_IconLibrary_Individual_Navy_110419


UNCLASSIFIED

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



7/1/2025

UNCLASSIFIED

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY

Additional Information:

Definitions:

1. Counterintelligence: Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons or their agents, or international terrorist organizations or activities.


Source(s):

CI definition: DoD Directive 5240.02, "Counterintelligence (CI)", **Incorporating Change 1, Effective May 16, 2018** , Part II. Definitions.

Image: Stock.Adobe.com, image #792845930

UNCLASSIFIED

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!

7/1/2025

UNCLASSIFIED

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY

Additional Information:

Definitions:

1. Foreign Intelligence Entity: 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
2. Economic Espionage: Federal Bureau of Investigation (FBI) definition of Economic Espionage is foreign power-sponsored or coordinated intelligence activity directed at the

U.S. government or U.S. corporations, establishments, or persons, designed to unlawfully or clandestinely influence sensitive economic policy decisions or to unlawfully obtain sensitive financial, trade, or economic policy information; proprietary economic information; or critical technologies. This theft, through open and clandestine methods, can provide foreign entities with vital proprietary economic information at a fraction of the true cost of its research and development, causing significant economic losses.”


Source(s):

DoD FIE definition: DoD Directive 5240.02, “Counterintelligence (CI)”, **Incorporating Change 1, Effective May 16, 2018**, Part II. Definitions.

FBI Economic Espionage definition: <https://www.fbi.gov/about/faqs/what-is-economic-espionage>. “Economic espionage”.

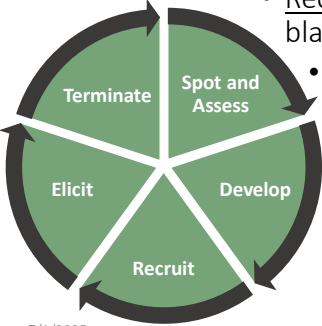
UNCLASSIFIED

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



7/1/2025

UNCLASSIFIED

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY

1. Spot and Assess a target with current or potential future access to key personnel or sensitive information, classified or unclassified, and identify exploitable characteristics unique to the target.
2. Develop a relationship with the target. Meetings become more private and less likely to be observable or reportable.
3. Recruit by appealing to ideology, financial gain, blackmail coercion, etc. These may manifest as observable and reportable behaviors.

4. Elicit information from witting or unwitting recruit.
5. Terminate activities or relationship.


CI awareness

Job Aid, Foreign Intelligence (FIE) Targeting and Recruitment”,

[https://www.dni.gov/files/NCSC/documents/Safeguarding
Science/foreign-intelligence-entity-targeting-recruitment-
methodology.pdf](https://www.dni.gov/files/NCSC/documents/Safeguarding%20Science/foreign-intelligence-entity-targeting-recruitment-methodology.pdf)

UNCLASSIFIED

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!

7/1/2025

UNCLASSIFIED

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY


1. “REMINDER: Foreign intelligence services often operate in countries other than their own, including those that are friendly to the U.S. You do not have to travel to an adversarial country to be targeted by a foreign intelligence service!”
2. “In the aftermath of several espionage cases, co-workers commented that they noticed unusual behavior, but did not know how to report concerns, or to whom.”
3. You do not have to travel to an adversarial country to be targeted by foreign intelligence services.

<https://www.cdse.edu/Training/Security-Shorts/CI022-resources/>

DNI, National Counterintelligence and Security Center (NCSC), “SEAD3 Awareness Briefing”, <https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-3-awareness-briefing.pdf>


UNCLASSIFIED

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



7/1/2025

UNCLASSIFIED

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY

Additional Information:

1. Direct elicitation: Suspicious questioning by translators, guides, and taxi drivers, or a pitch, (in-person or otherwise), requests to transport items, or exploiting criminal activities
2. Human targeting: coincidentally meeting someone who shares your interests at a public or professional conference or engagements, or a “Honeypot” ruse
3. Surveillance: Physical or electronic monitoring of your activities

CIA, Analyzing Economic Espionage, dated Spring 1992,
Approved for Release: 2014/09/10 C00622857,
https://www.cia.gov/readingroom/docs/DOC_0000622857.pdf


DCSA, CI Best Practices for Industry, Booklet, 17-09-12 CI,
https://www.dcsa.mil/Portals/69/documents/ci/17-09-12%20CI_Booklet_FINAL_web.pdf

DNI, NCSC: “SEAD3 Awareness Briefing”,
<https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-3-awareness-briefing.pdf>

Image: Stock.Adobe.com, image #76949467


UNCLASSIFIED

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 "Honeytrap" ruse



7/1/2025

UNCLASSIFIED

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY

Sources:

DNI, NCSC, "Travel Awareness" Brochure,

https://www.dni.gov/files/images/ncsc_toolkit/Travel.jpg


DNI, NCSC, "SEAD3 Awareness Briefing",

<https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-3-awareness-briefing.pdf>

Image: Stock.Adobe.com, image #92278099


UNCLASSIFIED


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 electronic 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





7/1/2025

UNCLASSIFIED

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY

Source(s):

DNI, Travel Tips web page, <https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-know-the-risk-raise-your-shield/ncsc-travel-tips>


<https://www.cdse.edu/Training/Security-Shorts/CI022-resources/>

Image: www.dvidshub.net, image #490577

Image: Stock.Adobe.com, image #251854983

Elicitation

UNCLASSIFIED




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.



7/1/2025

UNCLASSIFIED

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY

Additional Information:

Definition:

1. Elicitation is a technique used to discreetly gather information. It is a conversation with a specific purpose: collect information that is not readily available and do so without raising suspicion that specific facts are being sought. It is usually non-threatening, easy to disguise, deniable, and effective. The conversation can be in person, over the phone, or in writing. Conducted by a skilled collector, elicitation will appear to be normal social

or professional conversation. A person may never realize she was the target of elicitation or that she provided meaningful information.

Techniques:

1. Opposition / Feigned Incredulity: Indicate disbelief or opposition in order to prompt a person to offer information in defense of their position. “There’s no way you could design and produce this that fast!” “That’s good in theory, but...”
2. Provocative Statement: Entice the person to direct a question toward you, in order to set up the rest of the conversation. “I could kick myself for not taking that job offer.” Response: “Why didn’t you?” Since the other person is asking the question, it makes your part in the subsequent conversation more innocuous.
3. Questionnaires and Surveys: State a benign purpose for the survey. Surround a few questions you want answered with other logical questions. Or use a survey merely to get people to agree to talk with you.
4. Quote Reported Facts: Reference real or false information so the person believes that bit of information is in the public domain. “Will you comment on reports that your company is laying off employees?” “Did you read how analysts predict...”

5. Ruse Interviews: Someone pretending to be a headhunter calls and asks about your experience, qualifications, and recent projects.
6. Target the Outsider: Ask about an organization that the person does not belong to. Often friends, family, vendors, subsidiaries, or competitors know information but may not be sensitized about what not to share.
7. Volunteering Information / Quid Pro Quo: Give information in hopes that the person will reciprocate. "Our company's infrared sensors are only accurate 80% of the time at that distance. Are yours any better?"
8. Word Repetition: Repeat core words or concepts to encourage a person to expand on what he/she already said. "3,000 meter range, huh? Interesting."

Source(s):


DNI, NCSC, "CI Tips, Safe Travels" brochure, <https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-security-executive-agent/sead-3-toolkit>.

FBI, "Elicitation" brochure, <https://www.fbi.gov/file-repository/elicitration-brochure.pdf/view>

Image: Library of Congress, image #2022685327

Elicitation

UNCLASSIFIED



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!

7/1/2025

UNCLASSIFIED

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY

WHY ELICITATION WORKS

1. A trained elicitor understands certain human or cultural predispositions and uses techniques to exploit those. Natural tendencies an elicitor may try to exploit include:
2. A desire to be polite and helpful, even to strangers or new acquaintance.
3. A desire to appear well informed, especially about our profession.
4. A desire to feel appreciated and believe we are contributing to something important.
5. A tendency to expand on a topic when given praise or encouragement; to show off.
6. A tendency to gossip.
7. A tendency to correct others.
8. A tendency to underestimate the value of the information being sought or given, especially if we are unfamiliar with how else that information could be used.
9. A tendency to believe others are honest; a disinclination to be suspicious of others.
10. A tendency to answer truthfully when asked an “honest” question.

11. A desire to convert someone to our opinion.

For example, you meet someone at a public function and the natural getting-to-know-you questions eventually turn to your work. You never mention the name of your organization. The new person asks questions about job satisfaction at your company, perhaps while complaining about his job. You may think, “He has no idea where I work or what I really do. He’s just making idle chat. There’s no harm in answering.” However, he may know exactly what you do but he relies on his anonymity, your desire to be honest and appear knowledgeable, and your disinclination to be suspicious to get the information he wants. He may be hunting for a disgruntled employee who he can entice to give him insider information.


Shorts/CI022-resources/
<https://www.cdse.edu/Training/Security->

DNI, NCSC, “SEAD3 Awareness Briefing

FBI, “Elicitation” brochure, <https://www.fbi.gov/file-repository/elicitation-brochure.pdf/view>


UNCLASSIFIED

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



7/1/2025

UNCLASSIFIED

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY


<https://www.cdse.edu/Training/Security-Shorts/CI022-resources/>

FBI, "Elicitation" brochure, <https://www.fbi.gov/file-repository/elicitation-brochure.pdf/view>

Image: Stock.Adobe.com, image #642212702

UNCLASSIFIED

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!

7/1/2025

UNCLASSIFIED

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY

<https://www.cdse.edu/Training/Security-Shorts/CI022-resources/>

FBI, “Elicitation” brochure, <https://www.fbi.gov/file-repository/elicitation-brochure.pdf/view>

Personal Safety

UNCLASSIFIED



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



7/1/2025

UNCLASSIFIED

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY

Shorts/CI022-resources/

<https://www.cdse.edu/Training/Security->

Image: www.dvidshub.net, image #5629029

Personal Safety

UNCLASSIFIED



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



7/1/2025

UNCLASSIFIED


DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY

<https://www.cdse.edu/Training/Security-Shorts/CI022-resources/>

Image: Stock.Adobe.com, image #281416166


UNCLASSIFIED

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



7/1/2025

UNCLASSIFIED

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY

<https://www.cdse.edu/Training/Security-Shorts/CI022-resources/>

Image: DCSA_IconLibrary_Individual_Navy_110419

UNCLASSIFIED

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!

7/1/2025

UNCLASSIFIED

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY

<https://www.cdse.edu/Training/Security-Shorts/CI022-resources/>


DOS, Travel.State.Gov,
<https://travel.state.gov/content/travel/en/i>

nternational-
travel/emergencies/terrorism.html

Image: www.dvidshub.net, image
#1230952

UNCLASSIFIED

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

7/1/2025 UNCLASSIFIED DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

<https://www.cdse.edu/Training/Security-Shorts/CI022-resources/>


DOS, Travel.State.Gov,

<https://travel.state.gov/content/travel/en/i>

nternational-
travel/emergencies/terrorism.html


UNCLASSIFIED

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



7/1/2025

UNCLASSIFIED

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY

Shorts/CI022-resources/

<https://www.cdse.edu/Training/Security->


DOS, Travel.State.Gov,

<https://travel.state.gov/content/travel/en/international-travel/emergencies/terrorism.html>

Image: Stock.Adobe.com, image #121051055

UNCLASSIFIED

Personal Safety



Anomalous Health Incidents (AHI):

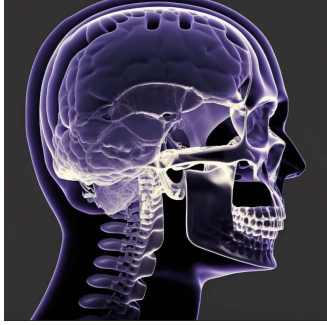
- Sudden onset of unexplained, unprompted events of sensations of sounds, vibrations, heat, or unexplained physical discomfort

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



7/1/2025

UNCLASSIFIED

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY

The information on this slide was coordinated with the Office for the Under Secretary of Defense Policy and the DIA CIAR Functional Manager.

Additional Information:

Anomalous Health Incidents:

1. Anomalous Health Incidents are also known as “Havana Syndrome.” They’re rare conditions that first occurred in 2016. Employees of the U.S. Embassy in Havana, Cuba, described sudden unexplained head pressure, head or ear pain, dizziness, and more.
2. In recent years, other federal employees reported a series of sudden and disturbing


sensory events. The scientific community's understanding of AHI is still evolving. The Department of Defense (DOD) is committed to guaranteeing people affected by AHI get the right medical care as quickly as possible.

3. Symptoms can vary but may include:

- a. Dizziness
- b. Emotional distress
- c. Headache
- d. Hearing loss
- e. Insomnia
- f. Mild confusion
- g. Nausea
- h. Slowed thinking

Additional Information: Anomalous Health Incidents | Health.mil, <https://health.mil/Military-Health-Topics/Warfighter-Brain-Health/Brain-Health-Topics/Anomalous-Health-Incidents>


Image: Stock.Adobe.com, image #601196477

UNCLASSIFIED


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



7/1/2025
UNCLASSIFIED

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY

1. Federal Trade Commissions, Consumer advice, <https://consumer.ftc.gov/identity-theft-and-online-security/online-privacy-and-security>

OSAC, July 2015, “Traveling With Mobile Devices: Trends & Best Practices”,

https://www.cdse.edu/Portals/124/Documents/jobajds/industrial/Traveling_with_Mobile_Devices_Trends_and_Best_Practices.pdf


DNI, NCSC, Fortify Electronic Devices, “CI Tips, Safe Travels” and “Mobile Safety” brochures, <https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-security-executive-agent/sead-3-toolkit>.

Cybersecurity and Infrastructure Security Agency (CISA), 12 June 2024, “Passwords”, <https://www.cisa.gov/secure-our-world/use-strong-passwords/>.

Image: DCSA_IconLibrary_Individual_Navy_110419

UNCLASSIFIED

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

7/1/2025

UNCLASSIFIED

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY

Source(s):

Federal Trade Commissions, Consumer advice: <https://consumer.ftc.gov/identity-theft-and-online-security/online-privacy-and-security>

DNI, NCSC, “CI Tips, Safe Travels” brochure, <https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-security-executive->

agent/sead-3-toolkit.

OSAC, July 2015, “Traveling With Mobile Devices: Trends & Best Practices”,

https://www.cdse.edu/Portals/124/Documents/jobaids/industrial/Traveling_with_Mobile_Devices_Trends_and_Best_Practices.pdf

UNCLASSIFIED

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

7/1/2025

UNCLASSIFIED

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY

Additional Information:

1. Transmitting sensitive government, personal, or proprietary information from abroad is therefore risky.
2. Security services and criminals can also insert malicious software into your device through any connection they control. They can also do it wirelessly if your device is enabled for wireless. When you connect to your home server, the "malware" can migrate to your business, agency, or home system, can inventory your system, and can send information back to the security service or potential malicious actor.
3. Security services and criminals can track your movements using your mobile phone or PDA and can turn on the microphone in your device even when you think it's off. To prevent this, remove the battery.

Federal Trade Commissions, Consumer advice: <https://consumer.ftc.gov/identity-theft-and-online-security/online-privacy-and-security>

DNI, NCSC, “CI Tips, Safe Travels” brochure, <https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-security-executive-agent/sead-3-toolkit>

OSAC, July 2015,
“Traveling With
Mobile Devices:
Trends & Best
Practices”,

https://www.cdse.edu/Portals/124/Documents/jobaids/industrial/Traveling_with_Mobile_Devices_Trends_and_Best_Practices.pdf

DNI, Travel Tips Web Page,

<https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-know-the-risk-raise-your-shield/ncsc-travel-tips>

Image: Stock.Adobe.com, image #267969101

UNCLASSIFIED

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/>.

7/1/2025

UNCLASSIFIED

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY


<https://www.cdse.edu/Training/Security-Shorts/CI022-resources/>

DOS, Travel.State.Gov,
<https://travel.state.gov/content/travel/en/i>

nternational-
travel/emergencies/terrorism.html

UNCLASSIFIED

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

7/1/2025

UNCLASSIFIED

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY

<https://www.cdse.edu/Training/Security-Shorts/CI022-resources/>

DOS, Travel.State.Gov,

<https://travel.state.gov/content/travel/en/international-travel/emergencies/terrorism.htm>

UNCLASSIFIED

Before You Go



Additional Resources:

- U.S. Department of State (DOS): [Travel \(state.gov\)](https://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 \(cia.gov\)](https://www.cia.gov/the-world-factbook/countries/)
- Federal Trade Commission: [FTC Online Privacy and Security](https://consumer.ftc.gov/identity-theft-and-online-security/)
- Office of the Director of National Intelligence (ODNI): [DNI SEAD3 Toolkit](#)



UNCLASSIFIED

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY

7/1/2025

DOS: Travel (state.gov) (<https://travel.state.gov/content/travel.html>)

1. Travel advisories, messages, and Alerts
2. Passport, VISAs, restrictions, vaccinations
3. Embassy contacts, website, and address
4. Smart Traveler Enrollment Program (STEP)
5. Health information and COVID restrictions

Countries - The World Factbook (cia.gov) (<https://www.cia.gov/the-world-factbook/countries/>)

Federal Trade Commission Online Privacy and Security, (<https://consumer.ftc.gov/identity-theft-and-online-security/>)

security/online-privacy-and-security)

DNI, SEAD3 Toolkit, (<https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-security-executive-agent/sead-3-toolkit>)

Image: Stock.Adobe.com, image #129986643

UNCLASSIFIED

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](#)



UNCLASSIFIED

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY

7/1/2025

CDSE:

1. Counterintelligence (cdse.edu),
<https://www.cdse.edu/catalog/counterintelligence/Federal/>
2. Counterintelligence Awareness Toolkit (cdse.edu),
<https://www.cdse.edu/Training/Toolkits/Counterintelligence-Awareness-Toolkit/>
3. FSO Toolkit (cdse.edu),
<https://www.cdse.edu/Training/Toolkits/FSO-Toolkit/>
4. Traveling with Mobile Devices: Trends and Best Practices (cdse.edu),
[https://www.cdse.edu/Portals/124/Documents/jobaid s/industrial/Traveling with Mobile Devices Trends and Best Practices.pdf?ver=PONp0mR5hblG_mSz4S7CXW==](https://www.cdse.edu/Portals/124/Documents/jobaid%20s%20industrial/Traveling_with_Mobile_Devices_Trends_and_Best_Practices.pdf?ver=PONp0mR5hblG_mSz4S7CXW==)


CI and Insider Threat Directorate:

1. SEAD 3 Unofficial Foreign Travel Reporting,
<https://www.dcsa.mil/Industrial-Security/National-Industrial-Security-Program-Oversight/SEAD-3-Unofficial-Foreign-Travel-Reporting/>
2. DCSA Reports, Flyers, Posters, and Handouts,
<https://www.dcsa.mil/Counterintelligence-Insider-Threat/>

Image: www.dvidshub.net, image #7630367


UNCLASSIFIED

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!

7/1/2025

UNCLASSIFIED

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY


1. Report Foreign Contacts:
 - a. With a known or suspected foreign intelligence entity.
 - b. Continuing association with known foreign nationals that involve bonds of affection, personal obligation, or intimate contact; or any contact that involves the exchange of personal information. This requirement applies regardless of where or how the contact was made (personal contact, Internet, etc.).
 - c. Following initial reporting of the contacts, updates regarding continuing unofficial association shall occur only for significant changes in the nature of the contact.
2. Individuals are still responsible for reporting suspicious interactions, activity or unexpected events when traveling or meeting foreign nationals for official business.
3. Foreign intelligence services often operate in countries other than their own, including those that are friendly to the United States. You do not have to travel to an adversarial country to be targeted by foreign intelligence services.

DNI, NCSC, “SEAD3 Awareness Briefing”,
[https://www.dni.gov/files/NCSC/documents/Regulations/
SEAD-3-awareness-briefing.pdf](https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-3-awareness-briefing.pdf)

Image: DCSA_IconLibrary_Individual_Navy_110419

UNCLASSIFIED

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!

7/1/2025

UNCLASSIFIED

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY

1. Required reporting related to cleared personnel, to include adverse information, should be reported via the DoD-designated personnel security system of record. The Defense Information System for Security (DISS) is the current DoD system of record for personnel security management.

DNI, NCSC, “SEAD3 Awareness Briefing”,
<https://www.dni.gov/files/NCSC/documents/Regulations>

/SEAD-3-awareness-briefing.pdf

UNCLASSIFIED

Questions?

Contact Information:

Jim Lyon
Integritys Corporation FSO
Office: (858) 300-1644
Cell: (623) 680-5641
E-mail: lyon_jim@integritys.com



7/1/2025

UNCLASSIFIED