



Overseas Defensive Travel and Counterintelligence Brief

Department of Commerce
Office of Security



Security & Safety Recommendations

- The security and safety measures suggested here will help to protect you from crime, terrorism, and actions by foreign intelligence and security organizations while traveling for the government.
- The level and type of threat varies from country to country and time-to-time, so you will need to pick and choose or modify these suggested security measures to meet your needs.

Forewarned is forearmed!



Defensive Travel



Country Specific Threat Updates

- The Department of State (DOS), Bureau of Consular Affairs maintains travel warnings and Consular Information Sheets with rules and regulations pertaining to foreign travelers for every country in the world at:
 - <http://www.state.gov/travel/>
- Classified, country-specific threat briefs can be arranged through the DOC's Office of Security.



Pre-Travel Wallet Preparation

- Check your wallet or purse and remove all credit cards, Social Security card, and other items not needed during your trip.
 - Do not take **unessential** papers, such as a military reserve ID.
 - Include an **Emergency Information Card** which has your name, blood type, known allergies, required medications, insurance information and emergency contact information.



Smart Copies and Carry-on Luggage

- Make copies of your passport, air tickets, all credit cards and any other documents that you will take to facilitate reporting their loss and replacing them.
- Carry **all** your prescriptions (in their original bottles), an extra pair of eyeglasses/contacts, a change of clothes and your personal document copies in your carry-on luggage.



Your Luggage

- Use **hard**, lockable luggage with a **TSA approved lock** (deters petty intrusion) and, **closed** name tags (prevents casual observation).
- Your luggage tags should show **only** your name, phone number and complete address.
- Do **not** use your business card as a luggage tag or display any logos, stickers or seals on your luggage which could **disclose an affiliation**.



Understanding the IT Threat

- First, understand the threat is real. Examples of reported incidents include:
 - Unauthorized full disk copies have been made while the laptop owner was out of the hotel room on overseas travel.
 - Laptops have been stolen at security screening lines at airports.
 - Wireless access services have been monitored by third parties to gain information transmitted through WiFi service.
 - Malicious software installations have occurred to include:
 - Key logger software.
 - Virus, trojan horse and other malware has been installed on laptop computers which capture device log-in data and attempt to call “home” to pre-destined [non-DOC] location.



DOC IT Travel Policy

- Permanent-issued DOC laptops that connect to Operating Unit networks and personal laptops are prohibited from use while on official foreign travel.
- Only Operating Unit office-issued loaner laptops are authorized during foreign travel.
 - Loaner laptops should only be utilized on foreign travel when there is an official business need.
 - Using the loaner laptop, only remote access via Operating Unit internet based e-mail, or issued MobiKey will be permitted during foreign travel.



DOC IT Travel Policy

- Department of Commerce personnel must have their Blackberries evaluated before and after foreign travel by their Operating Unit for adequate security controls:
 - At least 72 hours prior to travel, and again within the first business day upon return, prior to connecting the device to a networked computer.
- OS Blackberry users with security clearances may contact 202-482-5344 to view a video on protective techniques.
- If your Blackberry is ever lost or stolen, immediately report the incident to your Operating Unit IT Security Officer.



Information Technology Security

- Make sure your use of Government Furnished Equipment (GFE) and Commerce data is used and secured in accordance with the Commerce IT Security Program Policy and Minimum Implementation Standards.
- Gain supervisory approval to remotely use and/or access information.
- Attend Commerce sponsored IT security awareness training to ensure you understand threats affecting the security of Commerce systems and data.
- Only transport electronic devices containing Federal government information (Government furnished equipment) when absolutely required for use during travel.
- If office staff travel frequently, consider setting up a community use laptop program for overseas use that is routinely disk-wiped to erase unnecessary data.
 - No sensitive data is authorized for storage on loaner laptops.



Information Technology Security (con't)

- Ensure information is “backed-up” prior to travel.
- Create strong and unique passwords, and shield passwords from view when inputting.
- Be aware of shoulder surfing when viewing device monitors or reading non-digital documents.
- Run up-to-date anti-virus, anti-spyware, and personal firewalls.
- Terminate connections when not in use.
- Clear browser history and cache after use, and close browser.
- Implement “full disk” encryption for portable electronic devices when traveling abroad.
- Maintain physical control of laptop computer and other electronic devices when traveling overseas (lock in hotel room safe only when you control the key).
- Consider using a cable lock to secure the mobile device to an immovable object.
- Don't put smaller, portable devices in back pockets, or unsecured luggage (such as an open pocket).
- Minimize the data stored on electronic devices used when traveling overseas.



Information Technology Security (con't)

- When using portable thumb drives for data storage, ensure that the device is secure using FIPS 140-2 encryption technology to protect data.
- Inventory what is loaded (software, data, etc.) on the laptop or other electronic devices prior to departure and after return from travel overseas.
- Do not loan your laptop to anyone while traveling abroad. An innocent connection to an IT system or website could result in malware being loaded on your computer.
- Minimize web-browsing while traveling overseas and when using a non-Commerce managed Internet web service.
- Do Not use overseas Wireless (WiFi) public use service to connect to Commerce systems, i.e., do not check your email or access DOC business systems using a WiFi service where sniffing or key-logging can take place.
- Disable the Infrared Port (i.e., cover it with a piece of black electrical tape, or disable via the BIOS) on portable electronic devices.



Reporting IT-Related Incidents

- It is Commerce policy that you report any incident relating to Information Technology, including data compromise and loss of equipment such as laptops, Blackberry, DOC issued cell phones, thumb drives etc...to your respective organization's IT Security Officer *immediately* after you confirm or suspect a compromise. You should note that you cannot wait until your return from travel to file a report. Your agency's Computer Incident Response Team will ensure that reported information is properly managed and addressed.



Pre-Travel Electronic Device Preparations

- Avoid taking laptops, cell phones, PDAs and other electronic devices (especially GPS capable), overseas unless specifically needed.
 - Consider taking copies or using a FIPS 140-2 secure/encrypted thumb drive or other storage media for digital data. You should make sure to secure the location where you keep your data to prevent easy access.
 - Many US cellular services are not accessible outside of North America.
 - **Special** country specific, electrical adaptor/converters may be needed to **safely** (surge protection?!) recharge these devices.
- Portable electronic devices are **regularly** targeted by thieves (cash value) and foreign intelligence services (information value).
- Some countries have **import restrictions** or **prohibit** the entry/use of encryption programs within their borders. Check the State Department website for more information U.S. Department of State International travel tips and travel warnings can be found at <http://travel.state.gov>.



Pre-Travel Laptop Preparations

- If you are taking a laptop or similar device:
 - Back up all files before leaving; take only what you need, **diskwipe** (not delete) the rest per DoD standards.
 - Keep only software programs on your laptop and store data files (especially sensitive ones) on a thumb drive or other storage media which you carry **separately**.
 - Disable the Infrared Port (i.e., cover it with a piece of black electrical tape, or disable via the BIOS) on portable electronic devices.
 - **NEVER** store passwords, sign-on sequences or access phone numbers on any laptop/device or in its case.



Pre-Travel Safety and Security Preparations

- To avoid attracting criminal interest; dress discreetly and **appropriately** to blend with the local culture, avoid the appearance of wealth and consider wearing no jewelry.
- Obtain a modest sum of foreign currency **before** you leave home; criminals watch for travelers exchanging large amounts of currency at airport banks or currency exchange windows.



Pre-Travel Safety and Security Preparations

- Prepare yourself for all possibilities.
- It seems impossible, but consider what would happen if you became a victim of a hijacking, kidnapping or other hostage situation.
- Are your personal affairs in order?
 - Do you have an up to date?:
 - Will with an “MIA clause”.
 - A Living Will.
 - Durable Power of Attorney for your Finances.
 - Durable Power of Attorney for your Medical Decisions.
 - Long-term child care or custody agreement.
 - Other important matters.



Terrorism Awareness

- Terrorism is the threat or use of violence by a person or group against civilians, their property or institutions with the intention of **intimidating** people and **coercing** governments for political or ideological ends.
- Terrorist methods include threats, bombings, kidnappings, hostage takings, hijackings, assassinations, sabotage, arson, armed raids or attacks and other actions to disrupt civil activities.



Terrorism Awareness

- Over the last 10 years, significant terrorist incidents have shown an **increasing** trend both in number and severity of attacks.
- In 1998, Osama bin Laden issued a public anti-American “fatwa”, or religious ruling, in which all Muslims were openly invited to undertake terrorist attacks against **American civilians** and allied interests worldwide.



Anti-Terrorism Awareness

- Anti-Terrorism is a collection of defensive measures implemented to **reduce the vulnerability** of people, their property and institutions from terrorist attacks.
- The threat of terrorism must be taken **seriously** by all Americans, **especially those who travel regularly**.
- All Americans should **intensify** personal security practices while on travel outside the U.S.
- See the Department of State's website for numerous international subjects, links to travel warnings and other related anti-terrorism information and links at:

<http://www.state.gov/>



Kidnapping/Hostage Survival Guidelines

- The chances of you being kidnapped or taken hostage are **small**. If it does happen, your chances of survival are **high**.
- Remember, you are of value to those holding you only if you are **alive**, and they want to keep you that way.



Kidnapping/Hostage Survival Guidelines...

- The **best** opportunity for escape is in the **beginning**, during the confusion of apprehension while you are still in public.
 - Do not struggle or try to escape unless you are *reasonably* **certain** of success.
 - Try to cause as much commotion as **safely** possible to draw attention to the situation. So, the authorities can be notified of your abduction and begin their search for you.
- Once abducted, your best defense is **passive cooperation**; follow instructions and do not resist or struggle.
 - Attempt to visualize the route being taken; make mental note of turns, street noises, smells, etc. and the time between points.



Kidnapping/Hostage Survival Guidelines...

- Your initial destination may be a temporary holding place before being moved **again** to a more permanent location.
 - Calm yourself mentally and concentrate on surviving.
 - You could be moved several times overall.
- If you are questioned:
 - Be polite and keep your temper, act **cooperative**.
 - Take a simple, tenable position and stick to it.
 - Give **short** answers and do **not** volunteer information.
 - Talk freely about unimportant matters, but be **guarded** about matters of substance.
 - Do not **antagonize** your questioner with obstinate behavior.



Kidnapping/Hostage Survival Guidelines...

- After reaching what you presume to be your permanent location:
 - Plan on a **long** stay. Establish a daily schedule of mental as well as physical exercise. **Eat** what you are given even if it does not look appetizing or you do not feel hungry.
 - Don't be afraid to ask for medicine.
 - Try to **establish a rapport** with your captors; to encourage them to view you as a real person – family, sports and hobbies are universal topics.
 - Ask them to teach you their language.
 - Once a rapport is achieved, try asking (in a reasonable, low-key manner) for items that will increase your personal comfort.



Kidnapping/Hostage Survival Guidelines...

- After reaching what you presume to be your permanent location:
 - Observe your surroundings, use all your senses; try to determine the layout (location) of your building/compound.
 - Study your captors; note how many, their names, physical descriptions, habits and organization. Memorize their schedule, look for patterns of behavior and identify weaknesses or vulnerabilities.
 - Use your new knowledge to assess opportunities to escape; do not attempt escape unless you are certain of success.
 - If you detect the presence of other hostages try to devise ways to communicate with them.



Kidnapping/Hostage Survival Guidelines

- Be **patient**, as hostage negotiations are often difficult and time consuming. Remember, your chances of survival **increase with time**.
- Most episodes of hostage-taking end with no loss of life or physical injury to the captive.
- If a rescue force moves to rescue you:
 - If you hear shots, **immediately take cover**.
 - Remain calm and **do not move**. You do not want to be mistaken for a kidnapper.
 - Follow **all** the instructions given by the rescue force.



Hijacking Survival Guidelines

- Hijackings are **extremely rare**, but they do happen.
- The takeover of an aircraft (or transport) may be noisy and chaotic or quiet and methodical with little more than an announcement by a crew member.
- Either way, **how you and others react** during the first few minutes of a hijacking could be crucial to the outcome.
- Guidance prior to 9/11 focused on avoiding violence and achieving a peaceful resolution. Since then, a **more active and aggressive reaction** to a hijacking has been discussed.



Hijacking Survival Guidelines

- As of this writing, **no** official guidance has been issued by the U.S. Government.
- The most appropriate reaction will take into account the purpose of the hijacking:
 - Is it a suicide mission, a publicity stunt for a political movement or an attempt to escape to another country?
 - **The obvious and significant challenge will be to accurately discern the hijacking's purpose, quickly enough, to react effectively.**
- Remember that all hijackers may not reveal themselves initially; some may wait **quietly** to react to events.



Hijacking Survival Guidelines

- Remember that hijackers will be extremely nervous and unlikely to behave reasonably or rationally.
- One wrong move by a hostage could easily set off a spate of violence.
- Guidance prior to 9/11 says to:
 - Stay calm and encourage others around you to do the same.
 - Do not challenge the hijackers physically or verbally.
 - Comply with their instructions.
 - Do not struggle or try to escape unless you are *reasonably* certain of success.



Hijacking Survival Guidelines

- After the initial seizure is complete:
 - Passengers may be segregated by citizenship, sex, race, etc.
 - Your passport may be confiscated.
 - If possible, give your tourist passport - if you have it.
 - Do not hide your passport, papers or possessions.
 - Your carry-on luggage may be ransacked.
 - The aircraft may be diverted to another country.
- The hijackers may enter into negotiations.
 - Passengers may be released/exchanged for fuel, landing/departure rights, food, water, etc.
 - Prepare yourself mentally and emotionally for a long ordeal with possible abuse, lack of food and drink and unsanitary conditions.



Hijacking Survival Guidelines

- Blend in with the other passengers and avoid eye contact with your captors; do not draw attention to yourself.
- If you are addressed or questioned:
 - Respond calmly and act cooperative; do not show anger.
 - Give short answers and do not volunteer information.
 - Do not try to conceal your nationality or other obvious data.
 - Avoid political and religious topics.
 - Give innocuous reasons for traveling and minimize the importance of your job.
 - Never admit to any accusations.
- If you or another passenger needs assistance, always solicit a crew member first – never approach a hijacker.



Hijacking Survival Guidelines

- If negotiations are successful, the hijackers may surrender to authorities, release all the hostages or simply abandon the plane without incident.
- If not, a rescue force will re-take the aircraft:
 - If you hear shots, immediately take cover.
 - Remain calm and do not move. You do not want to be mistaken for a hijacker.
 - If fire or smoke appears, quickly use the emergency exits.
 - Follow all the instructions given by the rescue force.
 - On the tarmac, if not directed, quickly move away from the plane and then towards the terminal or control tower.
 - You may be treated as a hijacker until your identity is confirmed.



The Criminal Threat

- In comparison to all other threats addressed, your greatest and most immediate threat to a safe trip is **common criminal activity**.
- While traveling abroad, you will frequently find yourself in unfamiliar places, not knowing the local customs and language. And, thus a promising target for **local** criminals who are always looking for an easy mark.
 - In some countries, the criminals are bold, regularly violent and all too common.



Crime Protection

- A little prior planning, regular use of good security and safety measures, awareness of your environment and some basic common sense can effectively protect you.
- **Trust your instincts! Do not ignore or rationalize a fear response. Act with it!**
- When properly informed, your actions can avoid or minimize many risks, and readily deflect the attention of criminals to **a more promising individual**, an **easier mark**.
 - The least well protected individual is the easiest mark.
 - Criminals seek the least well protected individual because they want to use the smallest effort to achieve the greatest return with a reduced risk profile.



Petty Theft

- Protect yourself against petty theft.
 - Keep your luggage within view or touch at all times.
 - At counters, place your briefcase/purse in front of you, on the counter, and lean your luggage against your leg.
 - Watch for distractions which could be used by a pickpocket or thief.
- Do not place small portable electronic devices in your pockets or unsecured (i.e., no zipper or clasp) pockets in luggage.
- If you are taking a laptop (or other expensive equipment):
 - Treat it like a wallet or purse; keep it with you as carry-on luggage, do not check it in.
 - Laptops have a very distinctive shape, consider carrying a non descript carrying case.



Laptops In Transit

- If you are taking a laptop (or other expensive equipment):
 - When going through security, place your laptop on the X-ray machine's belt **after** all the delays, in front of you, are resolved; if you are delayed while going through, keep an eye on your laptop.
 - Be sure the batteries are charged to clear security checks.
 - Never store your assigned electronic devices, including laptop computer, Blackberry or other electronic device(s) in an airport or station locker.
 - If new, bring some proof of ownership (with serial number) to avoid an import duty by U.S. Customs; or register it, and other like items, with Customs prior to departure.
 - If you must leave it a car, lock it in the trunk and out of sight.



At the Airport

- At the airport maintain a low profile; do not delay in the main terminal, go directly through the security after ticketing or to ground transportation after arrival.
 - If a security incident occurs, quickly take cover behind a solid object – like a pillar or stairwell and do not move.
 - Wait for the local security force to give the ALL-CLEAR and follow their directions.
- Airplanes, terminals and taxis are not appropriate places to discuss sensitive subjects.
 - Conversations can be overheard and documents easily read.
 - At least one friendly, foreign country is known to collect intelligence by bugging airplane seats.
 - Laptops and other portable devices with screens and audio are just as vulnerable.



Ground Transportation

- NEVER!, EVER! take a gypsy taxi; always use a common commercial taxi from an official stand, if possible.
 - Do not get out of your taxi before your luggage.
- Avoid making yourself a potential target, always rent a conservative automobile.
 - Carjackers, common and frequently violent in some countries, target upscale vehicles.
- When driving, plan your route.
 - Get maps and confirm the directions to your destination before leaving (the rental agency).
 - Drive defensively; avoid getting boxed in and keep an open out.
 - If threatened, do not be afraid to floor it to get away.



At the Hotel

- If possible, **stay with your luggage** until it is brought into the lobby. (When leaving, enter your taxi just before or as your luggage is loaded.)
 - Consider using the bellhop, which causes the Hotel to be liable for your property.
- In many countries, you will be asked to **surrender your passport** when registering at a hotel. This is a **routine** procedure, as hotels must submit a daily report to police on all registered guests.
 - **Be aware that this information may be reviewed by the local intelligence service.**
 - Don't forget to get your passport back at the earliest opportunity.



Room Security At the Hotel

- Use all of the locking devices on your room door. Ensure the locks on all sliding glass doors, windows and any connecting door function correctly.
 - Remember the hotel's emergency keys can override your room door's deadbolt locks.
- Do not advertise your absence with the "Please Service This Room" sign. When out, use the "Do Not Disturb" sign.
- Carry your room key with you at all times. Do not needlessly display it, or carelessly leave it on a restaurant table or at the swimming pool where it could be easily stolen.



Safety at the Hotel

- Do not use your name when answering the phone.
- Never accept packages at your room, nor open the door to workmen (or any other unknown person), to include hotel staff, without prior verification from the front desk.
- Keep your luggage locked whenever you are out. This will not stop a professional but it will keep the curious maid honest.
- Consider anchoring your laptop or other portable electronic device to a metal post or fixed object in the room with a cable, or use the hotel room's safe.
- At night, lock your passport and other valuables (laptop) in your luggage or room safe. This reduces the risk of mysterious disappearances while you are asleep or in the shower.



At the Hotel

- Documents and other storage media that could be of value to an intelligence service should be kept on your person **at all times**.
- Do not invite strangers to your room.
- Consider bringing a **flashlight**, emergency power and emergency lighting often do not exist in hotels in developing countries.
- Review a local map to become familiar with the area.



On the Street

- Ask the front desk for help with reading the local map, finding a location or getting directions.
- Travel in pairs or with others when possible. Walk confidently and do not take shortcuts or alleys. If traveling alone after dark consider taking a cab to your destination.
- Know the local currency.
 - Keep large and small bills separate to avoid displaying a wad of large bills when paying for trivial expenses.
- Inspect your credit card after each use to ensure it is yours. This credit card scam is not new.



On the Street

- If you are taking public transportation, have your destination address written out in the local language on a piece of paper.
- Choose a good stop that affords easy, well-lit access to your destination. It is better to walk a few extra well-lit, well-traveled blocks than to cut across potentially hazardous area.
- Assess the area of your stop or destination before you disembark a public transport, leave a station or get out of a car.
- Avoid parking in un-lit lots or along dark streets.
- Know how to work the local public telephones.
 - Write down emergency numbers and carry change for phone calls.



Street Crime

- It is a good idea to keep your wallet in a front pocket to make it more difficult for a pickpocket to pick.
 - Back packs, fanny packs, purses and other bags are **easy** to pick.
 - Consider carrying and using a **throw-away wallet** with some old, canceled credit cards and a little cash.
- **Never** resist an armed robber, it could **quickly** lead to violence; and **never** pursue a thief.
- In a front pocket, keep some small bills handy to quickly appease a mugger. If pressed for more, give-up your wallet.
 - If possible, gently toss the throw-away wallet near the mugger's feet and quickly leave in the other direction.
 - If the above is not possible and you do not enough much money, offer up something else like your jacket or watch.



Street Demonstrations

- Avoid street demonstrations.
- If you are overtaken by a street demonstration, seek refuge in the nearest, appropriate safe haven; such as a hotel or department store.
- Do not use underground transportation to leave the area.
 - If service is stopped, you could be stranded underground.
 - And, tear gas is heavier than air which means it will flow down to and collect in subways tunnels and sewers.



Major Civil Unrest

- In the event of a major civil disorder, stay in your hotel.
 - Do not watch the activity directly.
 - Watching it on a local TV station would be best.
 - Stay away from all windows, glass panes and glass walls because of the potential of flying glass from a possible explosion.
 - Stay away from all exterior walls, especially nearest to the disorder outside.
 - Move to an inside room which will provide greater protection from gunfire and the like.
- If an emergency evacuation is issued or you believe it might be prudent, advise the nearest U.S. Embassy/Consulate, or other friendly embassy, of your status and location.
 - Hire someone to take your note to the embassy if the phones are out.



Counterintelligence Awareness



Who's Doing What to Whom?

- The intelligence services of rival and friendly countries are now more active in collection operations against the United States than during the Cold War.
- America's role as the dominant political, economic, and military force in the world makes it the **Number One target** for foreign intelligence collection.



You Are the Target

- As an American government official with access to useful information, **YOU** could become the target of a foreign intelligence operation at any time.
- Depending on your assignment, the risk of becoming an intelligence target may be ever-present, but can greatly increase during foreign travel.



In the Line of Fire: American Travelers Abroad

- While traveling abroad, you are on the host country's home turf, where the intelligence and security services of foreign governments have many resources available.
- They can **monitor** and, to some extent, **control** the environment in which you live and do your work.



How to Protect Yourself

- Common sense and basic counterintelligence awareness can offer protection against attempts to collect classified, proprietary, privileged, and other types of sensitive material.
- **TRUST YOUR SECURITY INSTINCTS!**
- Use the travel tips that follow – they're for your protection.



Rules to Travel By

- Maintain physical control of all sensitive materials at all times. Hotel safes are not an option.
 - Keep your laptop computer and cell phone as carry-on baggage; never check them with other luggage.
- Hotel rooms, commercial airplanes, or other public places are rarely suitable to discuss sensitive information.
- Do not use your computer or facsimile equipment at hotels or business centers for sensitive matters.



How They Get It...

- Be prepared to experience attempts at obtaining valuable information from you, such as:
 - **Friendly discussions with local contacts** that assess whether you have valuable information, and if you are exploitable.
 - **Eavesdropping** or **shoulder-surfing**.
 - Seemingly normal **conversations that are contrived** to elicit valuable information.
 - **Covert interceptions** of your phone, fax or computer communications at any location.
 - Physical (shadowing) or technical (recording or tracking) **surveillance**.
 - **Covert entry** into your hotel, vehicle or other personal area.
 - **Overt theft** of your property.



If You Are Arrested or Detained

- Stay calm, maintain your dignity and do not do anything to provoke the arresting officers.
- Request to contact the nearest US Embassy or Consulate.
 - If you are refused, **continue** to make the request periodically.
- Do not admit to anything or volunteer any information.
- Do not sign anything; **politely** decline until the document can be examined by an attorney or representative from the US Embassy or Consulate.



Reporting Security Incidents

- When overseas, security incidents should be reported to the Regional Security Officer through the nearest US diplomatic facility.
 - Remember that telephone calls to the local American Embassy or Consulate may be monitored by foreign intelligence & security services.
- After returning from your trip, any suspicious or noteworthy incidents should be immediately reported to your organization's appropriate security component, and to the Office of Security.
- When in doubt, **REPORT IT!**



Office of Security

- Check the State Department website for more information. U.S. Department of State International travel tips and warnings can be found at <http://travel.state.gov>.
- Classified, country-specific threat briefs can be arranged through DOC's Office of Security.
- If you need further assistance:
 - For country-specific threat briefs, please contact the OSY Anti-Terrorism Division at OSYOCI@doc.gov.
 - Promptly report suspicious activity and security incidents to the OSY Investigations and Intelligence Unit at (202) 482-2452.



[Click here](#)

in order to receive credit for satisfactorily completing this training and to receive your certificate of completion.

You can also type or copy and paste the following link into your Web browser:

<https://securityexchange.osec.doc.gov/cgi-bin/qwebcorporate.dll?idx=7D5FEN>

