LIS SOLUTIONS MONTHLY NEWSLETTER DECEMBER 2022

FOREIGN TRAVEL AND REPORTING

The holiday season is here and millions of people are hitting the roads and skies to visit family and friends and enjoy their time away from work. At LIS Solutions, we want everyone to have a happy and safe holiday season. This is why we'd like to remind everyone about some key policies and provide some helpful hints from the Federal Communications Commission (FCC) to make your time away from work as stress-free as possible.

If you are traveling abroad this holiday season, reporting your foreign travel is required. Specifically, all personnel are required to report all personal, official, and unofficial foreign travel with their Security Personnel at LIS.

Reporting your foreign travel request informs your security professionals of where you are going, where you will be, and who you intend on seeing while abroad. Also, your security professionals are able to provide security awareness, training, briefings, and education that is specific to the country you will visit to maximize your safety. If you have any questions or concerns regarding a specific foreign country of visit, we recommend reviewing the following website: **https://travel.state.gov/content/travel/en/international-travel.html**

Also, you are encouraged to visit the following website: **https://travel.state.gov/content/travel/en/us-visas/visa-information-resources/list-of-posts.html**. Here, you are able to find the List of U.S. Embassies and Consulates for any emergencies that might occur during your travel.

Any unreported foreign travel may cause suspicion around national security, threats, risks, and vulnerabilities. You may be investigated and the result could be the loss of your security clearance. For more details on reporting requirements, they are outlined in Security Executive Agent Directive 3 (SEAD 3) per the NISPOM.

BEFORE YOU TRAVEL

When traveling internationally, remember that your mobile phone and other personal communications devices transmit and store your personal information, which is as valuable as the contents of your suitcase, and possibly more so.

We recommend that if you can do without the device, don't take it. The same is true of your data. Don't take information you don't need, including sensitive contact information. Back up all of your data, remove any non-essential information from your device, and leave your backup at home.

With anything you do bring on your travels, take proactive steps to secure your devices and your personally identifiable information (such as your name, address, date of birth, and Social Security Number). In addition, you should:

- Back up your electronic files.
- Install strong passwords.
- Confirm antivirus software is up to date.

LIS Solutions
Analyze. Inform. Empower.

718-237-8919 • info@lissol.com

WHILE TRAVELING

Be vigilant about your surroundings and where and how you use your devices. Make sure to:

- Keep your devices secure in public places such as airports, hotels, and restaurants.
- Take care that nobody is trying to steal information from you by spying on your device screen while it's in use.
- Consider using a privacy screen on your laptop to restrict visibility.

Always consider the consequences of having your information stolen by a foreign government or competitor.

WHEN YOU GET HOME

Electronics and devices used or obtained abroad can be compromised. Your mobile phone and other electronic devices may be vulnerable to malware if you connect with local networks abroad. Update your security software and change your passwords on all devices on your return home.

SECURITY TIP: WI-FI THREATS

Some threats – device theft, for example – are obvious. Others, though, will be invisible, such as data thieves trying to pick off passwords to compromise your personally identifiable information or access your accounts. You may be especially vulnerable in locations with public Wi-Fi, including internet cafes, coffee shops, bookstores, travel agencies, clinics, libraries, airports, and hotels. Some helpful tips:

- Do not use the same passwords or PIN numbers abroad that you use in the United States.
- Do not use public Wi-Fi to make online purchases or access bank accounts.
- When logging into any public network, shut off your phone's auto-join function.
- While using a public Wi-Fi network, periodically adjust your phone settings to disconnect from the network, then log back in again.
- Try purposely logging onto public Wi-Fi using the wrong password. If you can get on anyway, that's a sign that the network is not secure.

Remember also to avoid using public equipment – such as phones, computers, and fax machines – for sensitive communications.

SOURCE
https://www.fcc.gov/consumers/guides/cybersecurity-tips-international-travelers

SECURITY TIP: REMAIN VIGILANT

When traveling, if you do encounter unexpected foreign contacts, foreign officials, or foreign personnel; they are to be considered "SUSPICIOUS CONTACTS" and you should be on the lookout for "SUSPICIOUS INDICATORS." If you have an encounter with a suspicious contact and have presented suspicious indicators, please report the following to your LIS Security Team immediately:

The essential facts of the incident:

- Who?
- What?
- When?
- Where?
- Why?
- How

LIS Solutions
Analyze. Inform. Empower.
718-237-8919 • info@lissol.com