Guidance for Employees Traveling to China
Issued November 6, 2023

The University of Arkansas desires to foster an academic environment in which scholarship and collaboration with colleagues internationally are encouraged and supported. Academic Policy 1835.00 International Travel of Students, Faculty, and Staff establishes baseline requirements for international travel, including China. However, there are special considerations for travelers to China, whether as employees or private citizens. This guidance sets out those considerations:

Why are there special considerations for travel to China[1]?

The U.S. Department of State considers China and Macau as "level 3" security risks. This means Americans should reconsider travel to these nations. Additionally, Hong Kong was identified as a "level 2" security risk and Americans should exercise increased caution when traveling there.

Travel to China requires registration of university-owned technology (laptop, tablet, cell phone, smartwatch, smartphone, PDA, or any other computing device issued by the university). This requirement was in place even before the June 30, 2023, advisory. Depending on the type of technology, an export control license issued by the federal government may be required for travel with such devices. The application process could take an undetermined number of months to receive a decision. Travelers should also be aware that China places restrictions on the use of certain encryption technology.

What should faculty, students, and staff consider before planning travel to China?

First, you should carefully consider the risk of detention by Chinese authorities outlined in the U.S. State Department advisory. When considering this, think about the type of work you plan to do while traveling and decide how you can travel as simply as possible.

Second, you should register your trip with the university and start the federal registration process for any device you plan to take as soon as possible (at least several weeks in advance) so there is adequate time to follow any potentially applicable federal laws and regulations. Make all required disclosures to the federal government and secure any required export control licenses as outlined below.

Third, delegate any tasks (e.g., Workday approvals) and set your university email to an automatic reply indicating you do not have access to email.

Fourth, ensure any device you take with you, plan to use or access while traveling does not have export-controlled software on it that is prohibited by any export-controlled country, including

[1] On February 13, 2023, the U.S. Department of State identified Russia as level 4 security risk or "do not travel". Until this changes, University employees will not be approved for travel to Russia.

China.[2] Please be aware that sanctioned and/or embargoed countries have export controls by the United States government. These may include travel to embargoed and/or highly sanctioned countries including Ukraine (Crimea - Donbas - Donetsk, Luhansk, Kherson, and Zaporizhzhya, and any other contested regions of Ukraine), Russia, Balkans, Belarus, China, Central African Republic, Congo, Cuba, Eritrea, Iran, Iraq, Lebanon, Liberia, Libya, Myanmar [Burma], North Korea, Somalia, Syria, Venezuela, Yemen, and Zimbabwe.

My university commitments make it necessary for me to go to China for university-related work and I want to access my email and documents while traveling. What do I need to do?

You may not take your university-issued technology to China. This includes a laptop, tablet, cell/smartphone, smartwatch, PDA or any other computing device issued by the University of Arkansas. You must use a loaner laptop specifically configured for travel to China, which is issued through University Information Technology Services (UITS). You must agree to its user terms, which includes basic cybersecurity measures intended to protect you and the university. Prior to traveling, you must also file a Federal Government Electronic Export Information (EEI) form ((EEI) filing) and include the submission confirmation in your Workday Foreign Travel Spend Authorization along with your Foreign Travel Export Control Form. If you have questions when registering your trip, contact University Export Control at exports@uark.edu and UITS at security@uark.edu.

Finally, with or without using a VPN, you will not have access to university systems (i.e., UAConnect, Blackboard, Workday, Streamlyne, or HPCC) while in China and should have an alternative plan. Travelers must not use their university credentials (i.e., username and password) to access UARK resources, including UA email or Box, while traveling. If you create a Yahoo account or similar for communication while traveling, be aware this account likely is not secure.

I've decided to go to China for university-related work (official business), and I plan to work with data sets and remote access to my research / scholarship files. What do I need to do?

You may not take your university-issued technology to China. This includes a laptop, tablet, cell/smartphone, smartwatch, PDA or any other computing device issued by the University of Arkansas. You must use a loaner laptop specifically configured for travel to China, which is issued through UITS. You must agree to its user terms, which includes basic cybersecurity measures intended to protect you and the university. Consult with University Export Control at exports@uark.edu and UITS at security@uark.edu to ensure the data you plan to use and the method to access it are both permissible under U.S. export control regulations and will be allowed by the university, considering cybersecurity concerns. There are controls and restrictions on certain software and hardware that may require a license in addition to the required EEI filing

[2] Find a complete and updated list of export controlled countries at the United States Department of The Treasury Office of Foreign Assets Control (OFAC) Sanctions Programs and Country Information; and the United States Department of State list of proscribed countries.

I'm planning to travel to China as a private individual (for vacation, for example). Do I have to register?

No, you do not, but we highly recommend registration of personal foreign travel with the U.S. Department of State Smart Traveler Enrollment Program (SMART). The university wants its travelers to be as safe as possible and registration can help us help you if you have issues. Even those engaging in private travel will be restricted in their use of university issued technology, systems, and data.

What if I travel as a private individual (on vacation, for example) and bring my own technology?

We do not recommend taking your own technology to China due to the security risks to you and the networks you may access while traveling. Additionally, returning home with technology such as a laptop, tablet, cell/smartphone, smartwatch, PDA or any other computing device and reconnecting to your home or work networks opens a broader community to risks (such as computer viruses) that can be avoided. Be aware that standard antivirus software may not detect when a device has been compromised.

If you absolutely can't travel without technology, consider buying a low-tech laptop and/or cell phone you can use and dispose of before leaving China or at once upon your return to the United States. Never connect that device to your home or work networks. Use the Yahoo account or similar technique noted above for essential communication.

We recommend you follow all federal laws and regulations and encourage filing any required documentation and ensure an export control license is requested if applicable. More information for personal travel recommendations may be found at the U.S. Department of Commerce Census Bureau and Export Administration Regulations.

What other steps should I take to enhance cyber and personal security?

- Tape-over, block, or obscure integrated cameras on the device.
- Physically disconnect or disable integrated microphones on the device.
- Install a privacy screen on the device to discourage so-called "shoulder surfing" where someone can easily read an unprotected screen "over your shoulder."
- Disable all file sharing.
- Disable all unnecessary network protocols (such as Wi-Fi, Bluetooth or infrared).
- Create a full backup of the device and any data before traveling in case the device is lost, stolen, seized or destroyed.
- Do not travel with unneeded door keys, smart cards, USB format PKI hard tokens, one time password crypto fobs, and similar access control devices.
- Be sure to clean out your purse or wallet, particularly if you normally carry notes about various accounts or passwords.
- If traveling with RFID cards (including U.S. Government Nexus "trusted traveler" cards), they should be carried inside an RF-shielded cover.
- If you need to send or receive email while traveling, create a temporary "throw away" account on Yahoo or a similar service before you travel.

- Do not use your regular email account.
- Do not send any sensitive messages via email.
- Avoid making or receiving voice calls, using voice mail, using IM or SMS, or sending or receiving faxes while traveling
- If you don't want to be geographically tracked, or you're trying to have a confidential, in-person conversation, batteries must be removed from cell phones. Even powered-off cell phones may be able to be turned into surreptitious monitoring and geolocation devices.
- Any/all CDs, DVDs, thumb drives, attachments, links and "QR" cell phone bar codes obtained while traveling should be considered potentially hostile and infected with malware.
- Do not use USB-based public battery charging stations; the USB interface to your device may allow the charging station to do more than just supply power.
- Do not buy new hardware while traveling that you intend to use upon return.
- Do not buy or download any new software while traveling.
- Do not have any of your electronic devices "repaired" or "worked-on" while traveling.
- Any discarded items (such as notes, documents, diskettes/CDs/DVDs) may be retrieved, analyzed and potentially exploited.
- So-called censorship circumvention tools (including Tor) may be blocked or supply imperfect anonymity; the use of such tools may attract official attention and result in you being investigated and punished or expelled.
- Guides, drivers, and interpreters may report on your activities.
- Beware of attempts to put you in embarrassing or compromising positions while traveling. You may be targeted for eventual extortion.
- If you are a U.S. citizen, register with the U.S. State Department's Smart Traveler Enrollment Program (step.state.gov) which notifies the nearest U.S. Embassy or Consulate of your travel plans. This allows you to receive vital information from the U.S. Embassy in China and connects you with the embassy in case of an emergency. It also allows you to report any suspicious incidents you experience to them. Nationals of other countries should investigate if their home countries provides similar services.
- If arrested, taken into custody, or interrogated, do not make any statements or sign any documents, particularly if they are written in a language you don't know. If you are a U.S. citizen, ask to have the U.S. Embassy or Consulate notified of your detention at once and to speak to a U.S. consular officer.