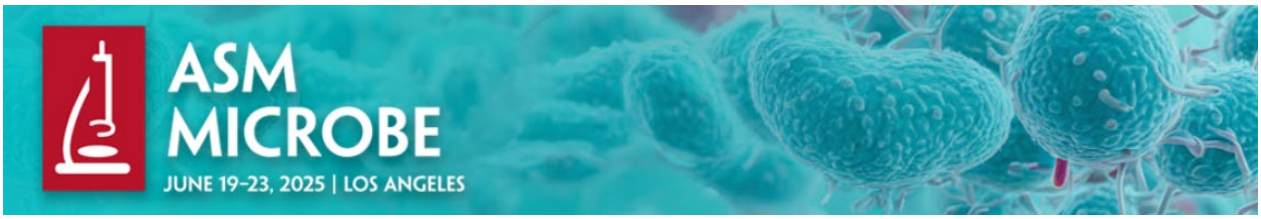

International Travel Guidance

Documentation for international travelers from non-restricted countries is often case specific based on the individual's circumstances. As a standard, all travelers should have a round trip ticket and hotel accommodations. All travelers must be prepared to state their purpose for travel, e.g. to attend ASM Microbe. An invitation letter is useful if put into secondary inspection for additional questioning.

Generally, international participants working in the US with green cards or valid visas may travel across state lines. If there are individual concerns, travelers should seek case specific advice from their institutions.

Individuals traveling from countries with travel bans:

- Nationals of the fully banned 12 countries (Afghanistan, Chad, Congo, Equatorial Guinea, Eritrea, Haiti, Iran, Libya, Myanmar, Somalia, Sudan, Yemen) cannot get new nonimmigrant visas—such as B-1/B-2 tourist visas—even if they meet usual criteria. Nationals of the partially banned 7 countries (Burundi, Cuba, Laos, Sierra Leone, Togo, Turkmenistan, Venezuela) are also barred from new B-1/B-2 visas.
- Individuals holding valid U.S. visas issued before June 9, 2025, may still enter—though they should expect heightened vetting by CBP at the border.
- Green Card holders from these countries or who traveled to these countries face no restrictions from the travel ban. However, even green card holders may face additional questioning, secondary inspection, or detainment at ports of entry, particularly if they've recently traveled to high-risk countries.
- Certain individuals not automatically exempt may apply for case-by-case waivers if they would suffer undue hardship without entry, pose no threat to U.S. security and have national interest justification. These often apply to business travelers with bona fide U.S. ties. Waivers are rare and tightly controlled and are unlikely to be timely.
- Those who've traveled to Iran, Iraq, Libya, Somalia, Sudan, Syria, Yemen after March 1, 2011, or to Cuba after January 12, 2021, are barred from using ESTA. ESTA (Electronic System for Travel Authorization) is a system that screens individuals before they travel to the United States under the Visa Waiver Program (VWP).

Guidance to help protect information and reduce risk while complying with applicable laws.

Individuals traveling internationally on behalf of an organization must note that U.S. Customs and Border Protection (CBP) has broad authority to inspect electronic devices—regardless of citizenship—at U.S. airports, land borders, seaports, and pre-clearance facilities abroad.

1. Understanding CBP Search Authority

• CBP may conduct warrantless searches of electronic devices under the “border search exception” to the Fourth Amendment.

Key points to know:

1 Basic searches (no suspicion required): CBP officers can ask to see the contents of your device—like photos, emails, or documents—without any suspicion.

2 Advanced searches (reasonable suspicion or national security concern): If they want to use forensic tools to copy or analyze data, they usually need reasonable suspicion or a national security reason.

3 Password requests: CBP can ask for passwords or access codes, though you can legally refuse. However, refusal could result in your device being detained or you being delayed or denied entry (if you’re not a U.S. citizen).

4 Device retention: CBP can temporarily seize your device for further examination, sometimes holding it for several days or even weeks.

• CBP has procedures for handling confidential business data, but protection is not guaranteed.

2. Cloud vs. Local Storage: Key Differences

• Local Storage: Data saved directly on your device can be accessed during CBP inspections—even in airplane mode.

• Cloud Storage: Stored remotely and generally only accessible if the device is logged in or syncing to cloud services. Use Airplane Mode: This prevents access to cloud-stored data, which CBP is not authorized to search.

Tip: Log out of cloud accounts and activate airplane mode before arriving at the border to limit access to cloud-based information. Officers may ask for passwords for your electronic devices. Courts have generally upheld CBP’s authority to search devices at the border but the law is still evolving, especially regarding encrypted or cloud-based content.

3. Preparation Before Travel

Evaluate Necessity

• Only bring devices essential to your trip.
• Consider using a dedicated travel device with limited data.
• If feasible, ship devices securely ahead of time.

Data Management

• Think of your device like a suitcase: bring only what you’re prepared to expose.
• Remove or encrypt any confidential or sensitive company files.
• Back up all important data to secure cloud platforms prior to departure.
• Consider a factory reset to protect private data.

Minimize Stored Data

• Avoid storing company documents or sensitive emails locally. Minimize Data: Carry only essential data. Consider using a “travel-only” device with minimal personal information. Backup and Remove Sensitive Data: Back up important information and remove sensitive data from your devices before travel.
• Empty “Trash” or “Recycle Bin” folders to ensure deleted files cannot be retrieved.

Device Security

• Use full-disk encryption with strong, unique passwords. Disable Biometric Unlocking: Use strong passcodes instead of fingerprint or facial recognition, as biometric data can be compelled.
• Power off your devices or use airplane mode before reaching the border.
• Disable automatic syncing and log out of applications that access cloud data.

4. At the Border

Know Your Rights and Risks

• U.S. citizens are not legally required to unlock their device, but refusal may result in device seizure. U.S. citizens cannot be denied entry; non-citizens may be denied admission. You cannot be denied entry to the U.S. for refusing to give a password—U.S. citizens have an absolute right to re-enter the country. However, CBP can detain your device for further inspection and may keep it for days or weeks. Refusal may result in increased questioning, delays, or flagging for future inspections.

• Unlike U.S. citizens, non-citizens do not have a guaranteed right to enter the U.S. (except lawful permanent residents, who have stronger rights). Refusing to unlock a device by a non-citizen and non-permanent resident could lead to denial of entry, visa revocation, as well as being turned away or detained, depending on the situation and immigration status and circumstances. Tourists, students, and temporary visa holders are especially vulnerable. Denial of entry can occur if CBP feels you’re not cooperating or if they suspect a violation of visa terms. Cooperating may avoid issues but raises privacy concerns.

• If your device contains confidential company information, politely state this to the agent.

• Do not share written passwords—enter them yourself if necessary.

• If an officer confiscates your electronic device, get a receipt and write down the officer’s name, agency, and badge number, along with the time and nature of any questions or searches.

Disclaimer: The travel guidance provided by the American Society for Microbiology is for informational purposes only and does not constitute legal or professional advice. While we strive to ensure the accuracy and relevance of the information shared, international travel regulations, health advisories, and entry requirements are subject to change without notice. Travelers are responsible for verifying all necessary documentation, visa requirements, and local laws applicable to their destination.

The American Society for Microbiology does not assume responsibility for any disruptions, delays, or unforeseen circumstances that may affect travel plans, including but not limited to government regulations, airline policies, safety concerns, or health-related issues. We encourage all attendees to consult official government sources, embassies, and travel agencies to obtain the most up-to-date guidance before making travel arrangements.

By relying on the information provided, travelers acknowledge that they do so at their own discretion and assume full responsibility for their travel decisions. The American Society for Microbiology shall not be liable for any consequences arising from the use of this guidance.