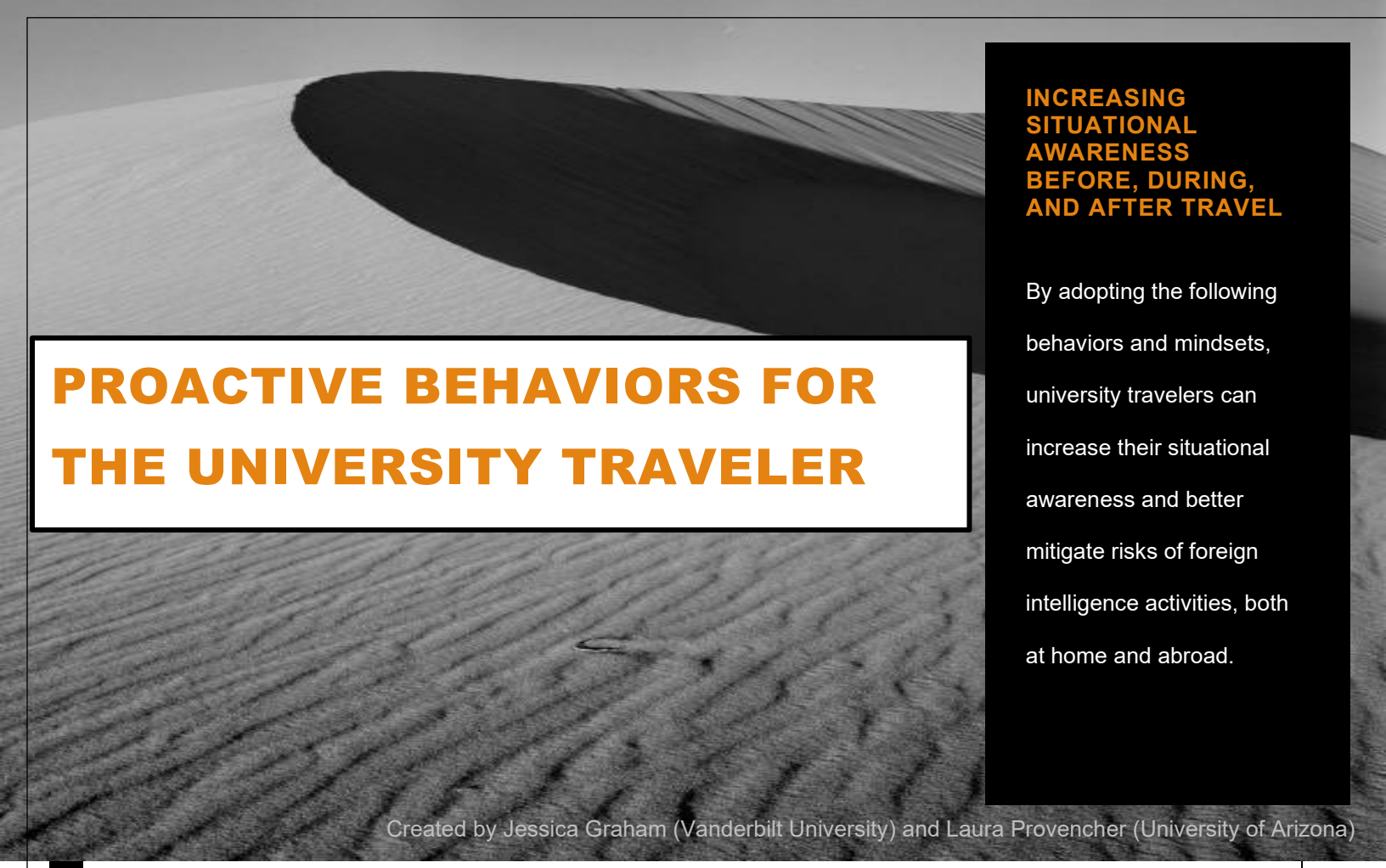

PROACTIVE BEHAVIORS FOR THE UNIVERSITY TRAVELER

INCREASING SITUATIONAL AWARENESS BEFORE, DURING, AND AFTER TRAVEL

By adopting the following behaviors and mindsets, university travelers can increase their situational awareness and better mitigate risks of foreign intelligence activities, both at home and abroad.

Created by Jessica Graham (Vanderbilt University) and Laura Provencher (University of Arizona)

In General

- ☐ Remain aware of your environment, don not let yourself become focused to the point of being unaware of what is occurring around you.
- ☐ Be comfortable saying “no”.
- ☐ Be selective in what you share; consider if something might be used against you or offer insights to you, family members, friends, colleagues.
- ☐ Understand how your work, experience, networks and connections (professional and personal), and/or aspirations may make you of interest to other countries.
- ☐ Recognize accepting LinkedIn requests provides information about your contacts, background, and professional reputation.
- ☐ Evaluate concerns and report suspicious contacts to your Facility Security Officer or other campus authority.
- ☐ Assess what you and others post on social media, blogs, or other open sources; this information can be used to learn a lot about you.
- ☐ Be cautious with casual acquaintances and suspicious of quick friendships. Notify someone of concerns, including suspicious contacts or requests.

Preparing to Travel

- ☐ Consult travel advisory and guidance for information about potential legal restrictions (e.g., requirements for use of VPN in China).
- ☐ Seek guidance from your institution’s travel and information security offices for general and country specific guidance, recommendations, and requirements. Use a “clean” laptop when available.

- Do not travel with sensitive, patentable, proprietary, restricted, or classified data.
- Minimize your digital footprint – wipe devices of any pictures, data, social media posts, or files that could be considered compromising.
- Assume everything that is emailed, posted, or accessed while abroad is not private.
- Prepare knowing you will be registered with the foreign government, and some governments may track you while you are in the country; your biometric data may also be recorded.
- Expect to have all devices, files, and pictures accessed and inspected.
- Update anti-virus software and establish firewalls for all devices.
- Create pass*phrases*, when accepted; if not, use complex passwords.
- Empty “trash” on laptops.

While Traveling

- Never use open and public Wi-Fi and do not assume Wi-Fi at lodging is secure.
- Avoid leaving electronics, passport, or documents where they can be easily retrieved during flight. Keep in mind that passengers in seats beside or behind you or walking by may be able to see your screen. (Enjoy a movie instead of working!)
- Keep in mind people – besides housekeeping – who may have access to your place of lodging; remember that hotel staff can access hotel safes!
- Avoid disclosing information about yourself, including travel plans and work, while in public places or using public transit like taxis or other hired vehicles.
- Do not access personal accounts (banking, retail, medical) or make purchases online.
- Use VPN; if illegal, consider not accessing anything online while traveling.
- Turn off Wi-Fi when not in use.
- Disable “remember me” and “history” functions, and file-sharing; manually enter your username and passwords for ALL apps.
- Do not download any apps or software updates.
- Do not click on links in emails.

Back Home

- Continue to monitor security of physical and cyber spaces at home and on campus.
- Take your laptop to IT to have scanned for malware, spyware, etc.
- Change your passwords immediately.
- Be wary of post-travel requests for unofficial consultations or technical or research advice (e.g., “opinion papers”); review requests for inaccuracies and inconsistencies.
- Be conscious of risks associated with accepting post-travel solicitations, gifts, or honors.
- Be mindful of your labs and research areas, who has access to them, etc. Report any strange occurrences taking place within.
- Report suspicious contacts to your Facility Security Officer or other campus authority.