Recommendations for Travelers to "High Risk" Countries or "High Sensitivity" Data

There are many good general recommendations for staying safe while traveling (see References below). This document is drafted with several specific recommendations to help protect Penn computer systems and data when you are traveling with highly sensitive data or to countries that may pose unique risks to computer security.

Two critical points before getting started: make sure you know your Local Support Provider (LSP – see References below) and be mindful that the most likely issue one encounters with a portable electronic device while traveling is loss or theft.

Things you really should do…

Before you go:

- Attend a Global Support Service awareness session on International Travel (see link below)
- Backup all data, and take only the minimum data necessary
- Work with your LSP to enroll in Penn's Two Factor service for PennKey: http://www.upenn.edu/computing/weblogin/two-step/. (***Make sure to print out sufficient single-use codes in case your phone is lost or stolen).***
- Work with your LSP on a methodology for remote identity proofing in the event that a device is lost or stolen and new credentials must be issued.
- Ensure best practices are in place for all mobile devices: encryption*, PIN or strong password protection, auto-lock after inactivity, auto-wipe after failed login attempts, device location services, and remote wipe.

While you're there:

- Avoid connecting 3rd-party USB and/or similar devices to your workstation
- Do not access systems or accounts that are not absolutely necessary
- Give preference to HTTPS for web services over HTTP
- Do not leave computers, phones and other electronic devices unattended (e.g., in hotel room) if at all possible.
- Use a Virtual Private Network (VPN) – work with your LSP to determine if there is already a recommended VPN solution in your School or Center. Otherwise, use ISC's service http://www.upenn.edu/computing/isc/lts/sras/

When you return:

- Change passwords
- Monitor accounts (requires working with your LSP and notification and/or registration of travel)
- Wipe & reinstall OS or restore from trusted backup. Carefully consider the transfer of any new data on to the restored system and scan before transfer.

Additional items that are nice to do, if you're able…

- *All the above, plus…*
- Work with your Local Support Provider to remove or restrict any elevated or sensitive permissions (e.g., root/super-user access, Group Policy Object permissions, etc.) while you are away.
- Talk to your LSP to find out if it is possible to bring and use loaned/dedicated devices with only the information you require for your trip.
- Consider whether or not it is feasible to use disposable (e.g., "burner") accounts for email, file sharing and any other required services
- Remember that not all internet connections are equal, and give preference to cellular over WiFi if available and coordinated with your provider in advance. Many carriers will rent a cellular WiFi hostpot that will allow you to use cellular data via WiFi. This is not only convenient, but it is safer than using other WiFi.

** Please note that you may be asked to relinquish or decrypt resources by local or national government officials.*

References:

ISC Data Security Travel Tips: www.upenn.edu/computing/security/advisories/InfoSec_Data_Security_Travel_Tips.pdf
Penn's Global Support Services website: http://global.upenn.edu/gss
Local Support Provider contact page: www.upenn.edu/computing/view/support/staff.html