

SECUR IT

The Care and Feeding of Laptop Computers

An increasing number of people who travel on Department business are taking portable computers (laptops or notebooks) with them. To ensure that you return intact the spiffy portable computer that you've taken, and to minimize security concerns while it's in your possession, here are some important points to keep in mind.

Rule # 1. Don't ever consign the laptop to the cargo hold of the aircraft. Yes, it's amazing, but true. Some people really do check their laptops. First, it will get stolen. It's happened many times to employees of this Department, and it will continue to happen. You get to where you're going, you rush down to the baggage carousel, and all you see is your battered old soft-sided suitcase with duct tape holding it together. No sign of the laptop. Guess what happened?

Second, some airlines depressurize their cargo holds (not many North American airlines do this, but who knows what Air Bujumbura does). If you've ever seen what this does to the nifty colour display on your laptop, you'll know it's unmistakable. You get a kaleidoscopic "wash" effect across the display, and the laptop is rendered useless. If you know anything about replacement costs for these things, you know that it's not worth it to have the screen replaced.

When you travel through airports with your laptop, you may wonder if you should subject it to X-ray machines. After watching "The X-Files" for a couple of years, we trust no one and recommend passing the laptop and diskettes (along with

camera and film) around the machine. We've been told by those who should know that there isn't much of an X-ray risk to magnetic media, but that the magnets used in the conveyer belts may be of some concern. Again, X-rays are probably not much of a risk in North America, but who knows how high they've got the machines cranked up at Botswana International Airport — hey, we're not even sure we should be walking through the darned things.

Airport security officials will probably want you to demonstrate that your laptop really is a laptop. At O'Hare International Airport a couple of years ago, we were asked to make the laptop "do something." We fired it up, and got the DOS prompt. "Not good enough," we were told. "Make it do something." Straining for a solution, we finally launched a solitaire game from within Windows. That met with their complete approval.

In the aircraft itself, the flight crew may ask you to stow your laptop during take-off and landing, because of the possibility that it may interfere with the aircraft's guidance systems. Do what they say.

When you get to where you're going, you should be conscious of two things: the need to physically safeguard the laptop; and the need to physically safeguard your data. These are two entirely separate concerns.

Rule # 2. Don't leave your laptop in your hotel room (if at all possible) and don't entrust it to the hotel safe.

Laptops are small enough these days that you can pretty much take them with you wherever you go — they'll fit in briefcases, large purses, etc. You can even make arrangements to leave them in a safe place at a mission, if you happen to be dealing with one in your travels.

Rule # 3. Store your data separate from the laptop. Always. That means on diskettes, and it means keeping the diskettes physically separate from the laptop. Don't put the diskettes in the handy-dandy pockets and pouches in your laptop carrying case — if your laptop is stolen, the diskettes will be too.

To illustrate the point, just ask the British military officer who left his laptop unattended in the car. When he returned, short minutes later, the laptop was gone — and so were tactical plans for troop movements in the Gulf War. Enough said.

Up to what level of information can be processed on a laptop?

As far as security guidelines go, you may process up to and including SECRET information on a laptop. For all intents and purposes, laptops do not emanate and are not therefore subject to TEMPEST requirements, regardless of geographic location (unlike ordinary desktop computers, which radiate like you wouldn't believe for a fair distance, and are therefore subject to TEMPEST requirements at missions abroad). You are not, therefore, required to have a TEMPEST laptop, as there just isn't any evidence of a credible threat against them from an Emanation Security (EMSEC) perspective.

Rule # 4. You must transit your data via some other, secure, system.

A final point

If you take a laptop on business, you are fully responsible for it. You must take reasonable, effective precautions at all times to ensure the safety of the Department's assets, whether physical, as in the case of equipment like a laptop, or intellectual, as in the case of information and data.