

# Don't Let Lack of Labels Leave You Liable

February 2008



## ON CYBER PATROL



Imagine you have two cabinets in your kitchen. One is labeled "Poisons" and the other is marked "Tasty Treats." OK, it's a strange kitchen. On the counter below are two identical containers. They are identical in every way – same weight, same size, and same appearance. Neither container is labeled. One of the containers is near the cabinet that says Poisons; the other is near the cabinet that says Tasty Treats. It might be a fair guess that the one near the Treats cabinet is just that – something good to eat. The other one must be for ratttraps.

However, you want to make sure, so you carefully open the container and take a whiff of the contents. Almonds! You like almonds and so you put them in your Tasty Treat Bowl and start chowing down. You spy and murder mystery buffs see where I'm going with this, don't you? For those of you too young to watch *Murder She Wrote*, arsenic has the smell of almonds. You suddenly stop munching those almonds in mid bite – but it's too late. Labels – correct and clear labels – would have been useful in this situation.

Let's move that same scenario into a room filled with computers. The cabinets become computers, some labeled Classified, some not. On the tables around them are CDs, DVDs, flash drives and other portable media all without labels. How can you be sure that the storage media that you plug into an unsecured machine does not contain proprietary data? Are you willing to "taste" them to be sure? The message here is simple: unlabeled and mislabeled storage media pose risks because of potential confusion, misuse and compromised security.

Unfortunately, inspections of classified electronic resources have turned up many such examples. For example, IA inspectors found two switches in a room -- one is classified, one is unclassified. The classified is plugged into the unclassified and unclassified plugged into classified. The reason? They were side by side and nothing was marked!

Paraphrased from Army regulations: labeling, marking, and controlling media: all personnel must protect and classify media inserted into a system at the highest level the system is accredited to process until the data or media is reviewed and downgraded by the Information Assurance Security Officer (IASO). It also makes sense that when media changes classification, it should be immediately and correctly relabeled.

The storage media available has increased its capacity and reduced its physical size to the point that huge amounts of data can be held in the palm of your hand. Not knowing what is on a particular disk or drive could lead to careless physical security measures. U.S. computer equipment is frequently for sale in the bazaars of the Middle East. Need we say more?

Marking and controlling portable media is as important as any other security measure. Even if there are additional safeguards such as encryption and password protection, labeling media correctly will prevent confusion and potential risk to classified data. Take those extra few seconds to mark that thumb drive or CD and make sure that the designation is clear and correct.