

USB's

February 2010



ON CYBER PATROL

As covered or mandat



Can technology counteract the determined, the deceitful and the dimwitted? This is a question that has yet to be answered as the Army and other branches look at resuming the use of flash media on military networks.

Recently, the Joint Task Force (JTF) opened the door for allowing the resumption of stored media technology via USB ports. This would reverse the policy change that came into effect approximately a year ago after network infiltration by malicious software residing on a flash device. Several Army organizations are taking a hard look at protecting its networks before allowing the resumption of flash use. Specifically they want to ensure that only government approved or provided media can be used and that systems and networks are configured to mitigate flash-borne threats effectively.

The banning of flash media, especially the popular and easy to use "thumb drives," has caused significant inconvenience among those who came to rely on the technology for the fast and easy movement of data between devices. Resumption of flash use will increase efficiency, and in a way increase security by reducing or eliminating the use of even riskier workarounds devised to transport data.

The question is, will all the safeguards in the eventual policy be enough? Portable media has been in use for a long time and the military had a wide ranging set of rules and regulations governing its use. The incidents that prompted the ban would seem to prove that those business practices were not enough. Many technical experts will tell you that technology alone can offer adequate protection. Yet technology is under constant assault from three threats – all human.

The first is the determined. The number of computer government networks containing proprietary data that have not been breached at some level makes up a very short list. If human intelligence can create technology, it can also devise a way to defeat it. The second is the deceitful. Technology can be compromised when intentionally not put in place fully and correctly --- by a human. All it takes is one compromised or conniving individual to bypass all the technology safeguards, if that person is at a critical junction in network security. Background checks are useful, but hardly foolproof. The third threat is the dimwitted. Throughout history, how many catastrophes have happened because logical, intelligent people have thought "nobody would ever do that!" For example, was the combined application of peanut butter and motor oil ever considered in flash media testing? While that particular example might not be an issue, something of that kind could well create a security compromise.

The Army will soon provide its guidance and policies of flash use. However, even with all the rules, regulations and technology that will go into the return of flash media on military networks, effective information assurance will still come down to responsibility, knowledge and attention. Those attributes will spell the difference between total security and potential disaster. The previously described threats can only be fully mitigated through thorough effective training, continuous communications and constant vigilance. The last element, vigilance, is perhaps the most crucial. Because when it all boils down, only individual actions can ensure effective security.