

National Aeronautics and  
Space Administration  
**Headquarters**  
Washington, DC 20546-0001



Reply to Attn of:

Office of the Chief Information Officer

JUN 2 2010

TO: ODIN Program Office

FROM: Deputy Chief Information Officer for IT Security

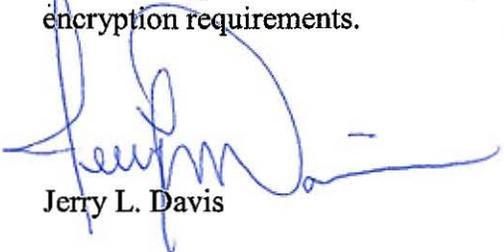
SUBJECT: Removal of Memory Stick Devices from the ODIN Enterprise Catalog

NASA has established encryption requirements for its information technology resources that store and process Sensitive But Unclassified (SBU) data. In accordance with NPR 2810.1, Security of Information Technology, "NASA management shall comply with NIST FIPS Publication 140-2, Security Requirements for Cryptographic Modules, FIPS Publication 46-3, Data Encryption Standard and NIST SP 800-77, Guide to IPsec VPNs."

On January 8, 2010 it was reported in numerous publications that certain memory stick devices once believed to meet the encryption requirements outlined in FIPS 140-2 had been found to actually fail FIPS 140-2 encryption requirements. The devices in question include the Kingston DataTraveler Blackbox, the SanDisk Cruzer Enterprise FIPS Edition, and the Verbatim Corporate Secure FIPS Edition.

The NASA Information Technology Security Advisory Board (ITSAB) has requested the ODIN Program Management Office to verify if any of the noncompliant memory stick devices are available on the ODIN Enterprise catalog. If any of the memory stick devices failing to meet FIPS 140-2 encryption requirements are available in the ODIN Enterprise catalog these devices are to be removed from the catalog.

Furthermore, consistent with the requirements in NPR 2810.1, no NASA SBU data may be stored or processed on memory stick devices which are not compliant with FIPS 140-2 encryption requirements.



Jerry L. Davis

cc:  
ARC/Ernest Lopez  
DFRC/Anthony Thomas

GRC/Les Farkas  
GSFC/Joshua Krage  
HQ/Greg Kerr  
JPL/Jay Brar  
JSC/Ted Dyson  
KSC/Henry Yu  
LaRC/Kendall Freeman  
MSFC/David Black  
NSSC/Dave Epperson  
SSC/Monti Muhsin