DEPARTMENT OF THE AIR FORCE

PACIFIC AIR FORCES

YOKOTAABGM33-01

10 May 2012

MEMORANDUM FOR ALL YOKOTA AIR BASE PERSONNEL

FROM: 374 AW/CC

SUBJECT: Use of Unauthorized USB Devices on Yokota Air Base Networks

Releasability: There are no releasability restrictions on this publication

This is a Yokota Air Base Guidance Memorandum immediately implementing guidance towards the use of unauthorized USB devices on Yokota Air Base Networks for all Yokota Air Base personnel. Compliance with this Memorandum is mandatory. Paragraph 3 of this memo contains prohibitions enforceable against the individual. Failure to comply with the order articulated in paragraph 2 by all Yokota Air Base personnel can subject the violator to all forms of available punishment to include UCMJ action under Article 92, Failure to Obey Order or Regulation. To the extent its direction is inconsistent with other Air Force Publications, the information herein prevails, in accordance with AFI 33-360, *Publications and Forms Management*.

1. The Yokota Air Base networks are vital to our daily operations and every individual must do all they can to ensure the security of this capability. In accordance with Network Tasking Order 2008-320-001B, *Suspension of Removable Flash Media*, November 2008, USB devices with flash memory such as thumb drives, digital cameras, MP3 players, etc., are prohibited from use on DoD networks.

2. Recent investigations indicate that this memorandum is being violated. In response, we have deployed software that will automatically detect and report the presence of any USB devices on our computer networks. If you have a government issued USB hard drive for your official duties, please contact the Wing Information Assurance Office to ensure it is properly authorized.

3. Personnel who violate this memorandum will have their network account suspended until they reaccomplish all Information Assurance and Information Protection training and obtain a signed letter from their commander requesting account restoral from the 374th Mission Support Group Commander. Furthermore, failure to comply may result in confiscation of unauthorized devices and/or punishment under the Uniform Code of Military Justice or equivalent civilian disciplinary system.

4. Let me be clear, compliance with this network security directive is everyone's responsibility. My point of contact for this memorandum is the Wing Information Assurance Office, 225-9000.

5. This memorandum supersedes the previous memorandum letter, same subject dated 9 Aug 11.

Ensure all records created as a result of processes prescribed in this Memorandum are maintained in accordance with AF Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at https://www.my.af.mil/afrims/afrims/afrims/rims.cfm.

The guidance in this Memorandum becomes void after 180 days have elapsed from the date of this Memorandum, or upon release of an AF publication incorporating the guidance, whichever is earlier.

WILLIAM M. KNIGHT, Colonel, USAF
Commander
374th Airlift Wing