U.S. Army Information Technology Agency (ITA)

Strategic Communication Message, November 27, 2010, ITA, Pentagon, Washington,

Creating Connections

ITA Notification:
Protection of Classified Information on DoD SIPRNet

On November 27, 2010 USCYBERCOM released Communications Tasking Order (CTO) 10-133. This directive is intended to further protect classified information on DoD SIPRNet. This notification is intended to inform stakeholders of the CTO -10-133 requirement to immediately disable the capability to write to removable media on the SIPRNet.

The use of removable media on the SIPRNet network to download (write) classified material is of great concern to senior leadership and has been banned as prescribed in USCYBERCOM CTO 10-133.

Current Situation:
Unauthorized data transfers routinely occur on classified networks using removable media and provide one method that the insider threat can use to exploit classified information. To mitigate this activity, all DoD organizations must immediately disable the write capability on all SIPRNet machines as a default setting using any and all feasible means.

Clarifying Guidance:
Removable media is defined as CD/DVD, Secure Digital (SD) cards, Tape, Flash Memory data storage devices, MultiMediaCards (MMC), removable hard drives, etc. Removable media defined in this CTO does not include items such as tape-disk backup or hard drive removal per Special Security Officer (SSO) Sensitive Compartmented Information Facility (SCIF) requirements unless these media are intended for distribution.

Specific Actions:
In order to be in compliance with CTO -10-133, today, 8 Dec, ITA will disable write capabilities to all SIPRNet systems it manages . The Executive Director, U.S. Army Information Technology Agency/ Designated Approving Authority (DAA) is the only authority that can approve any exception requests for critical mission functions that require this capability.

Organizations supported by ITA must provide ITA with the specific names of individuals and systems that require the capability to write to removable media to have it reinstated. This approval will be on a case by case basis with a validated mission requirement detailed to the DAA. Send all requests for exception to your IMCEN Requirements Analysis Division Customer Liaison (RAD CL). If you have an afterhours critical mission need please contact the Helpdesk for assistance at (703) 693-4337.

Information and Assistance :
We will keep you advised as information develops. For further information, please refer to the HOW2 website at: https://how2.hqda.pentagon.mil/portal/ss/