

ITX HBSS Configuration/Exemption

FRAGO 13 to JTF-GNO OPORD 05-01 and MCEN OP Dir 180-12, directs the full deployment of the Host Base Security System (HBSS) point product to attained asset awareness. In addition to the HBSS point products, the capabilities of Rogue System Detection (RSD) must be configured and implemented on each subnet.

Units conducting ITX training at 29 Palms are required to install HBSS on all workstations and servers connecting to the ITX NIPR/SIPR network.

ITX Units are to contact the 29 Palms G-6 at (760) 830-7141 to obtain two CDs (1) SIPR and (1) NIPR) with the appropriate files for installing HBSS on all workstations and servers (WIN/Linux systems).

NMCI Assets are not recommended on the ITX tactical networks. Units desiring to use NMCI assets on the tactical networks are required place the NMCI assets in deployed status prior to arriving. The HBSS agent on NMCI will need to be removed and reinstalled and redirected to the ITX ePO server for the duration of the training period.

Prior to connecting to the ITX network, units are to ensure the following requirements are met:

Identify two unit HBSS POCs with Name, Rank and phone numbers (local to 29Palms or cell phones that have service at Camp Wilson).

Rename workstations/servers using the following naming convention ITX, Unit and Billet (Examples: ITX013rdBn8thMarCO, ITX013rdBn8thMarCOC01, ITX013rdBn8thMarS3Admin).

Identify any NMCI assets being placed on the tactical network.

Identify device type/ip address of devices to be exempted (Routers/Switches, Taclanes, Printers, VOIP systems, ESX servers).

Ensure virtual servers on the ESX server have the HBSS installed. Virtual Servers are not exempted.

Ensure all devices connecting to the ITX network are assigned a static ip from the unit's assigned IP range.

Use of private IPs (169.xxx.xxx.xxx, 172.xxx.xxx.xxx) is not allowed.

Ensure DHCP on all devices is disabled.

Ensure IPv6 and any components thereof are disabled in network connections. IPv6 is not authorized on the MCCEN

Ensure Windows Firewall on the computers is disabled.

Ensure DOD root certificates are installed on all workstations using special applications. HIPS will block access to any web sites requiring DOD root certificates if the certificates are not installed.

Identify COC computers that have CPOF and C2PC installed as they will require exemption. HIPS will block CPOF and C2PC Outbound/Inbound traffic if not exempted.

Ensure that once HBSS is installed that the systems remain on the network; this will allow the device to collect updates from the ePO server.

After installing the DLP agent, a reboot is required, this will allow for the computer to communicate with ePO server.