Defense Security Service

Checklist for NISP contractors connecting to DoD networks regarding requirements of U.S. Cyber Command Directive 10-133.

The following voluntary checklist will aid cleared contractors in ensuring compliance with DSS guidance.

Step Number	Required Task(s)	Reference DSS Guidance Text	Completed	Completion Date
1	Upon receipt of DSS email, communicate to all employees who have access to SIPRNET at the facility that data transfers from SIPRNET are suspended until additional procedures are submitted by the facility and approved by DSS.	Direct all personnel to cease data transfers on SIPRNet unless approved by the DAA until adequate technical measures are put in place.	□	
2	Disable Write Capabilities. a) Modify technical settings to disable write capabilities. b) Confirm write capability is disabled through testing. c) Identify computers where "write capability will be disabled" and create a *compliance tracking form*. d) Document how write capabilities have been disabled and tested. Update compliance tracking form from step c. e) Set up audit process for maintaining compliance. *If Data Transfers are not performed make sure that all write capabilities are disabled and documented in (M)SSP. Steps , 4 and 6 are not applicable.*	Disable the "write" capability for all forms of removable media devices on all information systems connected to the SIPRNet as a default setting, using any and all feasible means. • Removable media is defined as CD/DVD, Secure Digital (SD) cards, Tape, Flash Memory data storage devices, Multi Media Cards (MMC), removable hard drives, etc. • Removable media defined in the CTO does not include items such as tape/disk backup, unless these media are intended for distribution. • Computer name and serial number that was used to create the removable media. For Windows systems, until HBSS is installed, maintain a manual compliance tracking mechanism for disabling write functionality	□	

Checklist for NISP contractors connecting to DoD networks regarding requirements of U.S. Cyber Command Directive 10-133.

Step Number	Required Task(s)	Reference DSS Guidance Text	Completed	Completion Date
3	Determine contractor personnel that require write capabilities re-enabled and create a list. Request Risk Acceptance Letter (RAL) from the GCA authorizing the identified personnel to write off SIPRNET Note: RAL letter can include the authorized list as an attachment for maintenance purposes. A new RAL letter will be needed when a new employee requires write capabilities. Attach updated RAL letter to the SSP and submit to ODAA for notification purposes using the normal process. Also, send the updated RAL to DISA via VMS.	Establish a program to appoint and account for authorized personnel responsible for conducting data transfers.	□	
4	Establish a log for documents transferred from the SIPRNET.	Maintain a logbook for any document transferred by the contractor and make available to DSS during security reviews: • Date/time of transfer • Document subject • Type of document • Size of document • Name of individual who the download is for • Name of individual performing the download • Computer name and serial number that was used to create the removable media.		

Checklist for NISP contractors connecting to DoD networks regarding requirements of U.S. Cyber Command Directive 10-133.

Step Number	Required Task(s)	Reference DSS Guidance Text	Completed	Completion Date
5	**Windows Systems Only (HBSS)** a. Contact the GCA to determine the steps necessary for long term implementation of HBSS, for inclusion in a POAM to DSS. b. If and when HBSS is implemented, configure for CTO-133. (Device Control Module, Rogue System Monitor and Policy Auditor) and document in "SIPRNET Transfer Procedure".	Coordinate with their sponsor to obtain HBSS Initiate and submit a Plan of Action & Milestone for implementing Windows Host Based Security System (HBSS) on all Windows systems connected to the SIPRNet	□	
6	***ONLY IF FLASH MEDIA WILL BE USED for Writing off SIPRNET*** Contact the GCA to determine steps necessary to install NSA's File Sanitization Tool (FiST) with Magik Eraser (ME). Include under POAM, if needed. a. Install and Confirm ability to scan Flash media with NSA's File Sanitization Tool (FiST) with Magik Eraser (ME). b. Document sanitization tool use in a "SIPRNET Transfer Procedure"	Scan all flash media transfers to or from the IS with SIPR connection using the NSA's File Sanitization Tool (FiST) with Magik Eraser (ME)….	□	

Checklist for NISP contractors connecting to DoD networks regarding requirements of U.S. Cyber Command Directive 10-133.

Step Number	Required Task(s)	Reference DSS Guidance Text	Completed	Completion Date
7	Submit re-accreditation request to DSS using the normal process that includes items from the steps above (Note 1): • SIPRNET Transfer Procedure attachment • RAL from GCA • List of named authorized transfer individuals • Sample compliance tracking form for ensuring no write-capability exists • Sample log book form • POAM for HBSS or HBSS configuration for CTO 133 • POAM for FiST with ME or procedures and configuration if installed.	Proceed with the installation of Windows HBSS …with SSP resubmission to odaa@dss.mil (per ISFO Process Manual) to initiate the reaccreditation process.	□	
8	Report to DISA (through VMS) that a program has been established to appoint and account for personnel responsible for SIPRNET data transfers.	…and report compliance to DISA in the Vulnerability Management System (VMS).	□	

Note 1. On receipt of the re-accreditation request DSS will process as normal and issue an IATO. Once all items in the POAM have been completed DSS will process for an ATO.
If HBSS is already implemented set an onsite date and process ATO.

Additional Comments: