

Host Based Security System (HBSS) Intrusion Prevention Course

CIN for CND-OSE (HBSS, SCCVI, SCRI):

- For the fleet: W-150-2102
- For NOC commands: W-150-2103
- For ONE-Net commands: W-150-2104

Overview:

Host Based Security System (HBSS) - the DoD-Mandated tool used to provide Intrusion Prevention services with behavioral and signature protection. HBSS also provides desktop firewall protection by providing a filter between the host and the network.

Use:

All traffic to and from the host is scanned at the packet level and reports to a centrally managed firewall policy on the HBSS console, which makes configuring and maintaining firewall policies on the network easier and less time-consuming.

Initial Training:

Initial training of HBSS is provided as pre-installation training on a virtualized training suite.

Initial training is provided live - instructor based. Instructors bring a Mobile training suite and train fleet and shore sailors on the entire CND suite - HBSS, SCCVI, and SCRI, while submarines and JHSV will receive only HBSS.

Initial training is only provided just before an installation. It's coordinated with the specific ship and provided on location (usually pulled into a classroom environment - not onboard)

Follow-on Training:

Follow-on (sustainment) training is provided by Interactive Courseware (ICW) on Navy Knowledge On-Line (NKO) -- future plan will integrate training into an F-school at Navy Center for Information Dominance (CID) but that may not happen until FY13.

Follow on training can be accessed via NKO – course ID: cndose-spawar-0001

Course Completions:

Training completion is tracked using a Course Identification Number (CIN). Students receive credit for attending and passing the initial training class on their Electronic Training Jacket (ETJ).

Records are updated about 2 weeks after the completion of the initial training - Students can view completion and tracking info by accessing their ETJ.

Eligibility for Training:

Initial training is targeted towards senior enlisted - **E-5 to E-9**.

Prerequisite for the course is **NEC 2780** (Students need to have a basic security understanding and system administrator understanding to fully understand this robust system)

**** NO "seat fillers" of E-1 to E-6 that are not *well qualified* ****

Officers are not targeted for this training. Information Assurance Managers are the highest level of which training will benefit. This training is directly targeted towards operators and maintainers - not management/leadership/oversight.

Well qualified DON Civilian *may* be eligible for the training. SPAWAR Institute is doing more research on if DON Civilians are eligible for the training, as any network security administrative or auditing jobs would fit - anything network security management role wise.

Well qualified Navy Contractors may be eligible to attend training. SPAWAR Institute provides an open invitation to FSETs to attend training based on seating availability.

Arranging Training:

SPAWAR Institute provides initial installation training in the form of Instructor Led Training (ILT).

Training is not provided at a standard training facility. SPAWAR Institute coordinates training to be held in available classroom facilities such as ATG and RMC commands with Mobile TTE (Tactical Training Equipment) when an installation for HBSS takes place.

The plan will change within the next couple of years - the follow on training will transition into a real schoolhouse sponsored by CID (not scheduled to happen until 2013 at the earliest).

Additional online HBSS training is available from the Virtual Training Environment at <https://www.vte.cert.org>.

Any additional questions may be directed to Susan Hood at susan.m.hood@navy.mil.