

Cyber and Physical Security Stand Down

Managers Checklists C-AD (P. Pile)

Managers will take the following actions.

Take attendance at all hands meeting and PII training and return attendance sheets to department/division Training Coordinator.

done

Gather responses from employee checklists and update organizations Excel spreadsheet.

Done – updates were done (or will be done when the on-line web site is accessible) on-line by the end user at:

http://intranet.bnl.gov/itd/reg/reg_form.asp

Verify and change, as needed, the owner and system administrator for each computer and list changes on Excel spreadsheet.

Done – where possible. Configuration/owner/administrator updates were, for the most part, not done on the spreadsheet but done on-line by the end user at http://intranet.bnl.gov/itd/reg/reg_form.asp. This way the ITD data base was updated, as it should be, by the end user.

Many (>200) computers were not listed on the spreadsheet. Most were behind the C-AD Operations Firewall. Where possible, the end users of these machines verified that they were compliant or brought them into compliance with the “Employee Checklist” items. Attempts were made to connect with the above ITD website to verify configuration data but, because of the firewall, the web site was not able to interrogate the system in question. Future exercises such as this should be conducted with an up-to date ITD list of computers that include those behind the firewall.

C-AD has several “Group” computers, ones with multiple users, each with individual passwords and no owner or assigned administrator. These computers have not yet been verified to comply with the checklist requirements. This will be done at a later date.

C-AD has two computers used as “Comfort” displays (AGS and Booster), neither have screen savers since their display is on all the time, otherwise they are compliant.

C-AD has a few computers that are old and rarely used and in the process of being upgraded to bring them into compliance.

Review and update list of UNIX, Linux, Macintosh systems that are not running currently supported operating system versions.

Done - not a large number, spreadsheets need to be updated

Identify rooms/spaces containing computers and/or network jacks where the only protection is locking exterior building doors.

Bldg 1005S, Rooms L2,L3,L4

Bldg 911B, Room 211 – no door

Bldg 905, open annex

Bldg 911B, room 242 (Network Jack)

Bldg 1005 Tech Shop

Gather list of computers containing protected PII.

We have 3 computers belonging to the secretarial staff containing protected PII. We are in the process of ensuring the files in question are properly encrypted

Identify in the comment column of the Excel spreadsheet any computers that could not be located or accessed

Done, See spreadsheet

Within 30 days, managers must accomplish the required actions with absent employees, recording when completed.

C-AD still has over 50 desktop computers that need to be verified that they comply cyber security guidelines.

Managers will report back to standdown@bnl.gov by 5:30 p.m. concerning the following items:

Return updated spreadsheet with marked up information.

Rooms/spaces containing computers and/or network jacks where the only protection is locking exterior building doors.

Return updated list of unsupported operating systems for UNIX, Linux, Macintosh.

❑ Other:

Computers (desktop) not on the list: ~220 C-AD computers were not on the spreadsheet. Compliance is not known for 22 as the owners are absent, 9 are not compliant with issues being resolved and 5 are non-compliant group computers, again with issues to be resolved.

In addition we have >100 computers that are on the network that are not desktop machines to be addressed at a later date.

The list of computers containing protected PII should be delivered in hardcopy and hand-carried to Mike Bebon's office, Building 460, and marked Official Use Only.