

## **Comments on Department's "Remove IT as a reportable condition" Project Plan**

General Statement – The plan should consider short-term goals separately from long-term goals. If there are immediate needs, categorize them as such. A long-term strategy will benefit the department in each of the areas within the plan by integrating IT security into the business processes of our systems. Every change to the strategy requires several years to implement fully.

-Item 177 - Disagree with creating C&A schedule as proposed (1/3 every year). C&A is already every 3 years or upon major change. The major change issue is being worked out in the CSWG. What would help is to have a calendar that systems could use to identify by when they will need C&A for a major system change. The Dept needs flexibility to meet the demands of the systems, not vice versa. A solution is to copy what other Department's do and have a standing multi-vendor BPA in place that systems can use to acquire C&A resources.

- Item 122 – Suggest not placing too much effort in updating the existing BLSRs until NIST completes its C&A guidance, specifically 800-53(a) and 60. The existing BLSR is sufficient for the short term and ED's whole C&A program will need reevaluation once NIST has completed its guidance.

- Plan Implementation suggestion – Create a committee/subcommittee structure (see Congress) to accomplish the items in the project plan. The full committee makes final decisions on each issue and discusses the need for sub groups, but the subgroups/committees do the grunt work, develop recommendations and present to the full committee. Each committee needs a charter (with timeline), a chairperson and part time members. This strategy allows broad participation across the agency, which will result in a smooth(er) implementation.

### **Additional comments**

Items 14 through 22: Only allowing 1 day for each task seems very optimistic

Item 24: Can you ever really "wrap up," ie "close," C&A? Meaning, don't you have to do it every 3 years? Maybe reword this.

Item 35: Don't we already have a straw man for this (the guide that Derek wrote)?

Item 37: Not sure this can be done in just 1 day.

Item 50: Can we have all our CAPS "developed" by Jan. 23 (ie, by next Friday)? Does "developed" mean "a very rough draft"?

Item 64: Does “complete” really mean “implement all actions identified in the CAP”—ie, address all findings in some way?

Item 91: Seems like a long time for this study.

Item 96: Maybe we should wait until the independent verification (item 77) has been completed before completing this task (Establish Dept. Security Standards), as the results of this verification could provide useful input into developing new security standards.

Items 116-119: Can these tasks really be completed in one day?

Item 130: Don't we have to wait until new standards are finalized (item 96) before we can update existing policies and procedures? Or are task 96 and 130 the same task (eg, the updated policies and procedures ARE the new standards)? Also, many of the inputs for task 130 will not be available until only 1 or 2 months before this task is due (meaning, there is not really 6 months to complete task 130). For example, if the findings of task 103 are significant, and task 103 is not completed until 5/7/04, this gives us less than 2 months to update all policies and procedures to reflect the results of task 103.

Item 177: Correct that it will take almost 5 months to develop a C&A schedule? Seems like a long time.

Item 187: Sorry, but I don't really understand what this task is—does it replace the existing process for ensuring IT security compliance (eg, C&A, IG audits, precert reviews, ST&E, IV&V)?