

## Task 3.1 Certification and Accreditation

### Task Overview

FSA systems will undergo certification and accreditation for the first time during CY 03. BearingPoint will assist the Security and Privacy team review certification packages, recommend improvements to the certification packages, and coordinate the submission of test packages to the Department's Certification review group.

### Task Details

FSA Certification and Accreditation will proceed along several paths:

- Preparation of the Xacta tool
- Direct support to system C&A teams to prepare for C&A
- Post C&A support to address remediations and POA&Ms

The process of tailoring the Xacta tool already has begun in earnest. We began our work by reviewing the extent OCIO has tailored the tool and what areas remain. The move to Xacta 4.0 will enhance our ability to tailor the tool for FSA and ED. The increased functionality in 4.0 may allow our team to bypass the update process with Xacta and instead adjust the tool directly. Our team reviewed 453 C&A security requirements and associated test procedures. We added test procedures to most of the security requirements, reworded those requirements that were unclear, and deleted duplicate requirements. OCIO is reviewing our work and will provide concurrence shortly.

#### Direct support to system C&A teams to prepare for C&A

C&A is a new process within FSA and the Department. FSA system personnel will need frequent guidance and support throughout the C&A process. The security and privacy team will need to respond to these requests in a coordinated and consistent manner.

We now have roles and responsibilities identified for all FSA systems. We have begun C&A kickoff meetings with several systems, exploring system boundaries and identifying next steps.

A portion of the assistance we will provide FSA system personnel is in the area of system boundary definitions. Although a constant challenge within FSA and the security community, system boundaries are critical to the C&A process. We provided each C&A team a system boundary worksheet and system component worksheet to assist them consistently document their system.

C&A requires the completion of several security-related documents. We will offer our assistance in reviewing and commenting on C&A documentation. Where possible, we will provide tools and checklists to the C&A teams to first review their documents for compliance themselves prior to submission to the C&A team.

During the uploading of information into the Xacta tool, C&A teams surely will have questions and issues that need rapid resolution. The security and privacy team will offer immediate "help desk" assistance to anyone requesting Xacta assistance. Our team will either answer the question or request assistance from the company hosting Xacta or Xacta itself.

The security and privacy team will interact with all FSA systems throughout the C&A process. We will devote extra attention on the three CIO systems. We will periodically meet or contact VDC, NSLDS, and SAIG personnel to observe their C&A status. Where necessary, our team will shift resources to assist these personnel complete their C&A objectives.

#### Post C&A support to address remediations and POA&Ms

Every FSA system will have numerous corrective actions after the certification group tests its system. The security and privacy team will assist each system create reasonable remediation plans and format these remediations into the POA&M format. We will assist system personnel address cost considerations, the benefits or drawbacks of certain mitigation strategies, and create realistic timelines to implement corrective actions.

Beyond the direct C&A support, we assisted in other areas related to C&A. We created a system retirement justification form for systems wishing to bypass C&A because their system was being retired. The form outlined the argument for retirement and provided insight into the rational for certifying and accrediting systems. BearingPoint also developed a point paper on C&A for the COO, Terry Shaw. The document explored the mandate for performing C&A and offered several alternative approaches to conducting C&A with the Department.

#### **Task Status**

We have completed our review of the C&A security requirements and are prepared to deliver our comments to Telos for inclusion into the ED template. We will continue our C&A kickoff meetings with FSA systems and work closely with OCIO to further refine the C&A rollout.