

Task 3.4 Working Group

Task Overview

The FSA Security and Privacy team participates in numerous FSA and Departmental Working Groups. We provide subject matter expertise and briefing materials as necessary to support the team. Participation in working groups will be limited to those meetings where contractor involvement is necessary.

Task Details

The FSA security and privacy team will need to participate in several working groups, either on a consistent basis or ad hoc. The team may participate in groups that address security training, incident response, critical infrastructure protection, contractor clearances, or any number of security related topics. We will need to contact the lead for each working group and discuss areas where our support may further the mission of the group. When requested, we will prepare briefing materials to support the security and privacy team.

To date, we have supported the Xacta C&A working group and the Incident Response working group almost exclusively. Our involvement in both working groups has been extensive, providing thought leadership, chairing meetings, and developing supporting documentation. As the year progresses our involvement in Department working groups most likely will increase.

We also now support the Configuration Management Working Group. Our role is to ensure that patch management is embedded in FSA's final CM Plan. In parallel, we are meeting with several patch management vendors to review each company's capabilities and their applicability to the FSA environment

Recently, we began working with a newly formed Critical System Working Group that includes participants from across Education. Our initial task from the group is to develop a methodology to determine the security evaluation process systems should undergo when making changes to its components or data. We completed a draft of this methodology and presented our findings the work group. Our work was extremely well received by the group. They have asked for additional work as a result. We hope to submit another draft early in 04 and then have the documents issued as policy by the Department.

Mod 1, Period 2

BearingPoint supported the Department's Security Standards Working Group by providing expert guidance on the implementation of FIPS 199 and 800-60. We assisted in the creation of the Department's new data sensitivity classification methodology and the new system inventory process. We helped the Department redefine its impact level designation's for Confidentiality, Integrity, Availability. The working group has incorporated many of our suggestions into the new Department standards.

BearingPoint also provided extensive support to the Department's Audit Resolution Working Group (ARWG) by developing a customized risk-assessment methodology; providing substantive comments on the subsequent risk-assessment worksheet based on the previously mentioned methodology; writing the first draft of a guide to Independent Verification and Validation (IV&V) of existing security findings; and providing client support for (and also attending) the

weekly ARWG meetings. BearingPoint also created a process flow diagram for determining whether findings would be subject to internal or external IV&V.

For the next period, BearingPoint expects to spearhead a major initiative to streamline and consolidate the current existing multiple tracking systems for IT security findings.

Mod 1, Period 3

The workgroups met infrequently during this period. However, BearingPoint completed the IV&V process guide, and also drafted a proposed numbering system for future audit findings. BearingPoint staff also provided substantive comments on the Department's "re" certification efforts.

Task Status

For Modification 1, this task is complete.