Applied Security Task Force

Charge and Scope:

The Information Technology Planning Board (ITPB) and the Common Systems Group (CSG) proposed the formation of the Applied Security Task Force to become an authoritative security resource for the campus.

The Office of Information Technology (OIT) and Academic Technology Services (ATS) will provide support resources for the Task Force, including: logistics, meeting coordination, web site development, technical representation, and operational oversight. Communications Technology Services (CTS) will provide incident-tracking and reporting, network operations coordination, and technical representation. As a distributed technology board that is representative of both academic and administrative operations, the CSG will review and approve plans and provide ongoing guidance and input to the task force.

The core of the Task Force will be IT professionals who work primarily for distributed units that do not have campus-wide responsibility. These individuals will also have security design and/or practical application of security methods as part of their current job responsibilities. The members of the task force will be compensated for four hours per week through a dual-employment or stipend staffing model, which will be flexible to accommodate differences in department employment practice and policy.

Applied Security Task Force Goals:

1. Become an authoritative security resource to the campus.
   - Design a way in which the team can work in an applied way to triage security incidents.
   - Become a resource for security-related issues, e.g., a task force looking into encryption.
   - Help units with security, e.g., penetration-testing or network reviews.

2. Develop a proposal for a fully funded full-time security task force team.
Priorities for the first three to six months:

1. Review, refine and adopt security-tracking response procedures.
   - Become the stewards of the adopted security-tracking response procedures and maintain, adapt, and enhance them on an ongoing basis.
   - Develop implementation guidelines for the Minimum Security Standards so as to ensure the adoption of the standards.
   - Become the stewards of the MSS standards and refine, maintain, adapt and enhance them on an ongoing basis.

2. Create a work plan for getting eEye introduced and used by the campus (with some scoping yet to be developed).
   - Use eEye as a product to proactively understand vulnerabilities on campus.
   - Help people make use of the identified tools.
   - Work with eEye to maximize benefits to both eEye and UCLA.

3. Review and refine the job description for the UCLA IT Security Officer, and play a role in the recruitment and selection process.