FISSEA 2006 Conference

Allen Crawley
Deputy Assistant Inspector General for
Systems Evaluation
U.S. Department of Commerce
March 20, 2006

IT Security Work Program

- Evaluate
  - Operating unit IT security program
  - General support systems and major application systems
  - Contractor information security
  - Computer incident response capability
  - Certification and accreditation packages
- Consult to improve system certification and accreditation packages

IT Security Is Improving

- Our earlier independent evaluations found numerous problems
  - IT security historically had not received senior management attention and support
  - Reflecting this history of neglect, pervasive IT security weaknesses placed sensitive systems at serious risk
- We have worked with Commerce's CIO and staff to promote improvements

Positive Impacts

- Increased senior management attention to IT security
- Improved
  - Department-wide IT security policy and program
  - Operating unit IT security program, practices, and controls
- Greater focus on system certification and accreditation

An Important Lesson

- Certification and accreditation is essential for effective IT security – it is not just a paperwork exercise
  - Helps ensure system security controls are comprehensive and appropriate
  - Helps ensure security controls are working as intended
  - Allows senior management officials to ensure cost-effective security measures

C&A Deficiencies

- Incomplete system descriptions
- Incomplete system component inventory in system security plans
- Lack of current interconnection agreements
- C&A was not conducted when major system changes occurred
- Ineffective and incomplete management, operational, and technical control testing

C&A Deficiencies

- Ineffective and incomplete system vulnerability scanning
  - Limited scope of testing
  - Limited capability of scanning tool used by one bureau
  - Lack of vulnerability analysis

C&A Deficiencies

- Because of testing deficiencies, remaining vulnerabilities could not be identified for authorizing officials
  - Testing did not provide reasonable assurance that controls were in place and operating as intended