Measuring Information Security

Observations of the GAO

Presented to the CSSPAB

June 2000

Audits to date have usually not required precise security measurement

- Most agencies have serious weaknesses
- Controls selected and purportedly implemented by agencies are often not effective
- Few gray areas

As security programs improve, more precise measurement will be needed

- To determine if security is good enough
- To determine if security is meeting agency-defined needs
- To determine if an agency's security posture is stronger or weaker than it was during a previous audit
- To compare performance among agencies

GAO Approach

- Determine the extent to which security is effective
  - To what extent has an agency established a risk management process that, if properly implemented, would result in effective security?
  - How effective are existing controls, based on independent tests?

GAO Approach

- Risks of evaluating security programs without examining/testing controls in operation
  - Security programs that are fairly well-documented but largely ineffective
  - Paperwork planning exercises that do not result in substantive considerations of risk and implementation of effective controls.

Levels of security

- GAO has not formally defined levels of security.
- However, the following categories one through four generally describe conditions we have observed.
- As yet, we have not identified an agency that meets level five.

1. **Ineffective security**:

- No entity components have effective security controls, and there is a high risk of material loss, disclosure of sensitive information, loss of data integrity, or disruption of critical operations. This level is characterized by either (1) a significant lack of adequate policies or (2) a lack of compliance with properly designed policies. (Material weakness)

2. **Uneven or partially effective security**:

- One or more areas of security (e.g., access controls, software change controls, service continuity) or agency components have effective controls. However, significant weaknesses in other areas preclude overall computer security from being effective. (Material weakness)

3. **Generally effective security**:

- There are few significant weaknesses that require management's attention. (Reportable condition)

4. Very effective security:

- Computer security is effective overall, despite a limited number of minor weaknesses.

5. **Fully integrated security program**:

- There is an ongoing cycle of risk management activities. All changes to the computer environment trigger a security risk assessment, and appropriate actions are taken to reduce risks to an acceptable level.