Computer Security:

Standards?
Recommendations?
Guidelines?

Ed Roback
Chief, Computer Security Division
edward.roback@nist.gov

June 11, 2002

Information Technology Laboratory
Computer Security Division

NIST
National Institute of Standards and Technology

Seeking the Board's Advice

Question for Discussion: *Should selected Protection Profiles (PP) be made into Mandatory Federal Information Processing Standards (FIPS)?*

What is a PP?
What is a FIPS?
What does "Mandatory" mean?
What are other options?
What are in best interests?
  Industry, Federal Agencies, Security

What does "Mandatory" mean?

- When an agency decides it needs *x,* (e.g., currently limited to cryptography for unclassified-sensitive), it must do so in a FIPS approved manner
- 140-2 Security requirements for Cryptographic Modules (and validated products requirement)
- Also cryptographic algorithms and methods
- Waiver can be made by the heads of departments and agencies

Other Options

- NIST Special Publication (SP)
- Subset – "NIST Recommendations"
- Not "mandatory and binding," but often used by auditors
- OMB guidance to agencies

Some Cons?

- Relatively slow approval/change process
- Conflicts may arise due to modifications to respond to public comment process
  - current PPs in development or USG recommended
  - Desire to be fully consistent with subset of basic to medium profiles
- Only appropriate for relatively stable technologies
- Cost of meeting standard & testing

Discussion

Should selected Protection Profiles (PP) be made into Mandatory Federal Information Processing Standards (FIPS)?