

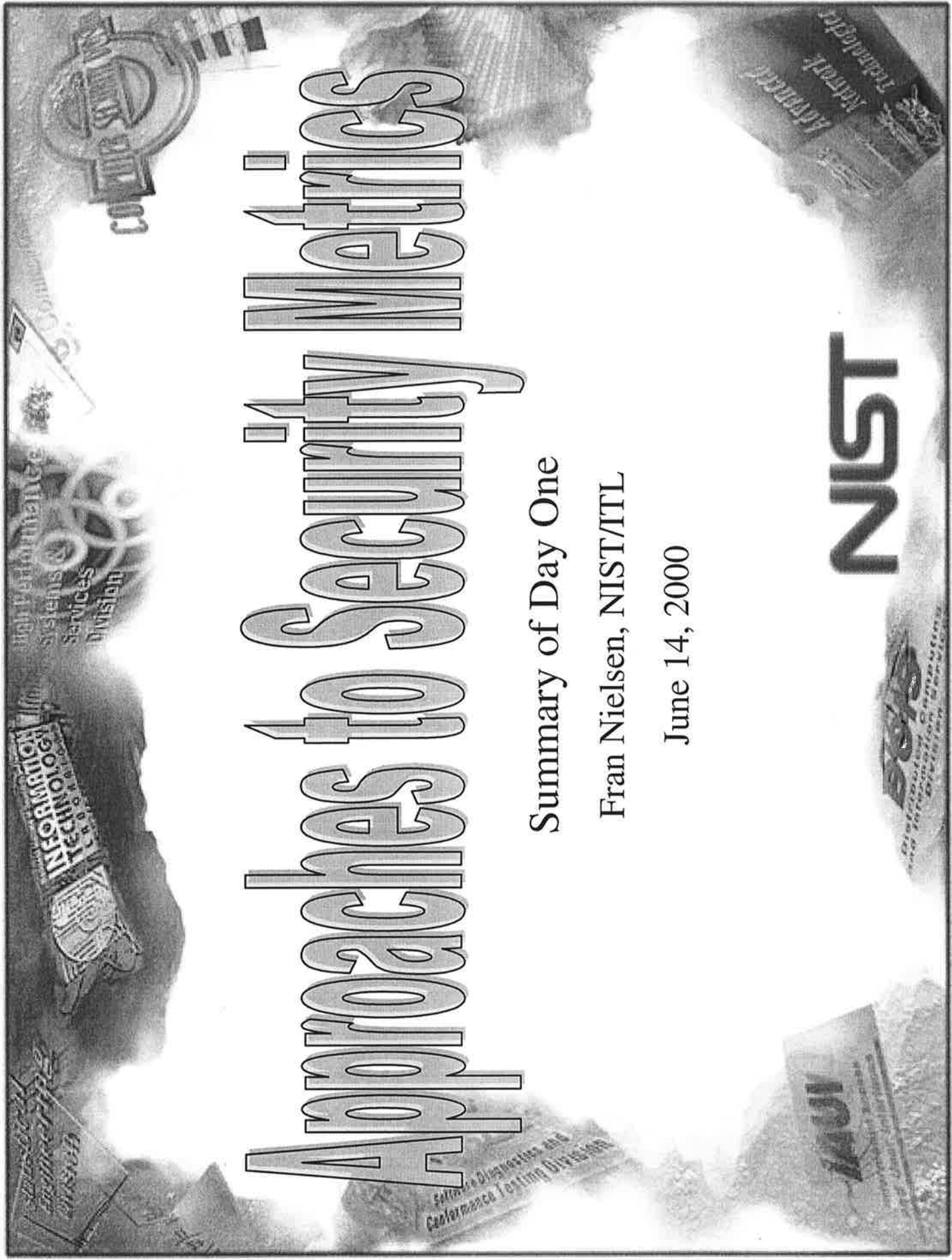
Approaches to Security Metrics

Summary of Day One

Fran Nielsen, NIST/ITL

June 14, 2000

NIST



What are Security Metrics?

- Katzke
 - set the stage
 - ambiguous, immature discipline, have different meanings
 - proposed a model showing the relationship of objects, security objectives, and the processes to measure them

IA Readiness Assessment

- Bartlett
 - designing an assessment process and pilot that is consistent, flexible, and relevant
 - using existence measurement points and integrating/aggregating results
 - 3 metric categories: people, operations & training, equipment & infrastructure

SSE-CMM PAM WG

- Jelen
 - Profiles, Assurance, and Metrics Committee, ISSEA
 - Overview of SSE-CMM appraisal as a metric
 - Two types of metrics
 - process - evidence of process maturity
 - security - extent to which security attribute is present

FISCAM

- Heim
 - Overview of FISCAM General Controls
 - Covers six control areas:
 - Security Program Planning/Management
 - Access Control
 - Application SW Development & Change Control
 - System Software
 - Segregation of Duties
 - Service Continuity

CIO's IT Security Assessment Framework

- Gilligan
 - high level tool meant to be relevant to management
 - leverages existing mandates and guidance
 - can be implemented now
 - 5 assessment levels: incomplete, complete, implemented, measured, pervasive

Audit-based Approach

- Bayuk
 - application of industry standard control objectives to a locally-defined systems security framework
 - uses audit steps as a basis for metrics
 - results in recommended improvements

Quantitative Risk Assessment

- Tompkins
 - risk analysis as a metric for determining security program effectiveness = “close enough”
 - planning is what’s important, not the plan
 - understand that it may be cheaper to “clean up” rather than have a strong security program
 - deal with the future no matter how much we know about the past

Cryptographic Metrics

- Smith
 - Summary and review of metrics for determining cryptographic strength

Concepts/Discussion Points

- What are we trying to achieve? Need something simple and effective that “tells the story”
- Sometimes we measure what we can measure.
- How can we measure something that keeps moving?

Concepts/Discussion Points

- Need a new paradigm - not systems and networks; think about enclaves and perimeters
- Measurements and metrics are different
- Metrics are not statistics - need correlation point to measure effectiveness

Concepts/Discussion Points

- Many dimensions of protection underlie the problem of defining/using metrics
- Need to differentiate between real new vulnerabilities and examples of vulnerabilities
- Can we move from subjective to empirically-based objective measures?