Security Framework Convergence

Bringing Communities of Interest Together

3rd Annual Security Automation Conference

September 19, 2007



Security Requirements Traceability

Legislation, Presidential Directives, OMB Policies 30.000 FT High Level, Generalized, Information Security Requirements **Federal Information Processing Standards** 15,000 FT FIPS 200: Minimum Information Security Requirements FIPS 199: Information System Security Categorization **Technical Operational** Management 5.000 FT **Security Controls Security Controls Security Controls Information System Configuration Settings Ground Zero Information Security Automation Program / Security Content Automation Protocol**

Unified Security Framework For Managing Enterprise Risk

The Generalized Model

Unique

Information Security Requirements

The "Delta"

Common

Information Security Requirements Intelligence Community Department of Defense

Federal Civil Agencies

Foundational Set of Information Security Standards and Guidance

- Standardized Risk Management Framework
- Standardized security categorization (criticality/sensitivity)
- Standardized security controls and control enhancements
- Standardized security control assessment procedures
- Standardized security certification and accreditation process

National security and non national security information systems



The Panelists

- Ron Ross, NIST (Moderator)
- Sherrill Nicely, ODNI
- Sharon Ehlers, ODNI
- Gary Guissanie, DOD
- Matt Scholl, NIST

