# Information Systems Security (ISS)

# Line of Business (LOB)


## John Sindelar
### General Services Administration


**Information Security and Privacy Advisory Board**
**Quarterly Meeting**
**September 14, 2005**

# Federal Information Systems Security Vision and Goals

**Vision:** The Federal Government's information system security program enables agencies' mission objectives through comprehensive and consistently implemented set of risk-based, cost-effective controls and measures that adequately protect information contained in Federal Government information systems.

## Goals

- Define and manage the federal government information security risk profiles
- Support performance of the federal government's mission through improved information sharing
- Establish a mechanism to acquire, distribute and support information security solutions
- Attract and retain a workforce capable of leading the confidentiality, integrity and availability of federal information and information systems

# Federal Information Systems Security Issues

**Security Training:**

- Wide divergence in cost
- Inconsistencies in meeting established standards
- Federal-wide standards for ISS skills have not been defined
- Lack of common criterion for credentialing ISS professionals

**FISMA Reporting:**

- Disparate and manual FISMA reporting processes within agencies tends to lead to inconsistent FISMA reporting

**Situational Awareness & Incident Response:**

- Uniform and comprehensive approach lacking within the federal government
- Agencies lack the knowledge, skills, and abilities to identify the vulnerabilities within IT infrastructure

**Security Solutions:**

- Lack of common methodology for evaluating security solutions and services

# ISSLOB Recommendations

- **Common Solutions** – to close ISS gaps by consistent and comprehensive implementation of proven security products, services, and training.
  - Address 4 areas: (1) Training; (2) FISMA Reporting; (3) Situational Awareness and Incident Response (SAIR); and (4) Security Solutions
  - Establish 3 Centers of Excellence (COEs) for each of the 4 areas
  - Phase-in of required and optional use of the common solutions in tiers over a 3 year period (except Training-Tier 1 which is 2 years)
  - Maintain agencies flexibility to tailor required solutions
  - Establish common metrics for effective performance evaluation

# ISSLOB
# Common Solution: Training

## Solution

- Common suites of ISS training products and training services for the Federal government, to include government-wide licenses

  - User Awareness - Tier 1 Required FY 07
  - Specialized Training - Tier 2 Optional FY 08

## Anticipated Outcomes

- Training that consistently meets all areas required by FISMA at a lower cost
- Development of Federal ISS skills, standards and competencies that align with nationally recognized credentials
- Infusion of ISS content into senior executive development and education programs
- Development of a repository of Federally-sponsored / approved COTS training products and sources

# ISSLOB
# Common Solution: FISMA Reporting

## Solution

- Provide agencies with shared products and services to comply with FISMA reporting requirements
  - Required - FY 07

## Anticipated Outcomes

- Government-wide process that can produce consistently standardized FISMA results to OMB and lower FISMA processing costs
- More efficient completion of the required annual security assessments and reporting, making it easier to keep information current for program management
- Efficiencies and cost savings including leveraged acquisitions through use of central, standardized tools

# ISSLOB
# Common Solution: Situational Awareness and Incident Response

## Solution

- Provide shared products and services for specific functional areas
- Expand enterprise level situational awareness and incident response capability

  - Tier 1 Required - FY 08
  - Tier 2 Optional - FY 09
  - Tier 3 Optional - FY 10

## Anticipated Outcomes

- Will complement not compete with existing CERT programs
- Affordable option for smaller agencies to be served by larger agencies without burdensome cost to maintain locally
- More uniform enterprise approach, as service will map to a standard method for conducting the activity, and improve consistency across Executive Branch

# ISSLOB
# Common Solution: Security Solutions

## Solution

- Partner with existing standards organizations to establish a process to guide agency personnel in selecting the appropriate security product or service

- Establish a repository containing:
  - Information on specific COTS / GOTS security solutions
  - Administrative procedures (risk management, cost benefit analyses, etc.)
  - Tier 1 Required FY 08
  - Tier 2 Optional FY 09

## Anticipated Outcomes

- Standardized methodology will provide for interoperability of security solutions and services, and ensure contractors and outsourcing providers follow the government's required baselines

# ISSLOB
# Center of Excellence (COE) Due Diligence Checklist

- Meeting NIST standards
- Business Process Support Strategy
- Shared Service Experience
- Demonstrated Customer Service Satisfaction
- Results of FISMA Reviews and FISMA Implementation Strategy
- Demonstrated Past Performance with Service Level Agreement
- Private/Public Strategy Plan
- Demonstrated Scalability Capability

# John Sindelar

**Project Director, Lines of Business**
**Deputy Associate Administrator**
**GSA Office of Governmentwide Policy**

John.sindelar@gsa.gov