

# ***Information Systems Security Line of Business (ISS LoB)***

**Information Security and Privacy Advisory Board**

**George Washington University**

**Washington, DC**

**March 22, 2007**

# Agenda

- Background
- Status
- Next Steps

# Background Lines of Business

---

## LoBs initiated in FY2004:

- Financial Management (FM)
- Human Resources Management (HR)
- Grants Management (GM)
- Federal Health Architecture (FHA)
- Case Management (CM)

## These LoBs have progressed:

- Common processes defined
  - Shared Service Centers established
- Due diligence validation in FM,HR

Common Solution: A business process and/or technology based shared service made available to government agencies.

Business Driven (vs. Technology Driven): Solutions address distinct business improvements that directly impact LoB performance goals.

Developed Through Architectural Processes: Solutions are developed through a set of common and repeatable processes and tools.

# Goals of ISS LoB

- Support performance of the Federal government's mission through improved information systems security
- Establish a mechanism to acquire, distribute and support information security solutions
- Leverage existing workforce resources capable of leading the confidentiality, integrity and availability of federal information and information systems and attract and retain supplemental workforce resources to this end

# Problem Statements

- Security Training:
- Lack of common ISS career path
- Federal-wide standards for ISS skills have not been defined
- Lack of common criterion for credentialing ISS professionals
- Agencies are individually developing and procuring baseline content and sustaining distinct infrastructure to support ISS
  
- FISMA reporting:
- Disparate and manual FISMA reporting processes within agencies tends to lead to inconsistent FISMA reporting to oversight organizations, and inadequate program management
- Gaps reflect lack of a cohesive government-wide approach to information security as well as the redundancy of existing information security processes
  
- 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 their IT infrastructure and the risk to their information resources
- Many agencies do not have technical or financial resources to mitigate these risks
  
- Lifecycle/Security Solutions:
- Lack of common mandatory methodology for lifecycle and security solutions and services
- Unnecessary demarcation of baseline requirements with respect to security solution selection for national security systems/information versus non-national security systems/information
- Lack of awareness of existing standards and/or guidance across the federal government for selection evaluation, testing, and acquisition of security solutions

# What the ISS LOB does not do

- Transfer accountability for agencies to meet all FISMA requirements and ensure an effective and efficient information systems security program
- Eliminate agency/program decision-making to integrate security products and services within the fabric of the agency's information security program
- Transfer resources for acquiring products and services to the SSCs except in those instances where agencies have agreed
- Intend that "one solution fits all" for agency security requirements

# Overall Task Force Recommendations

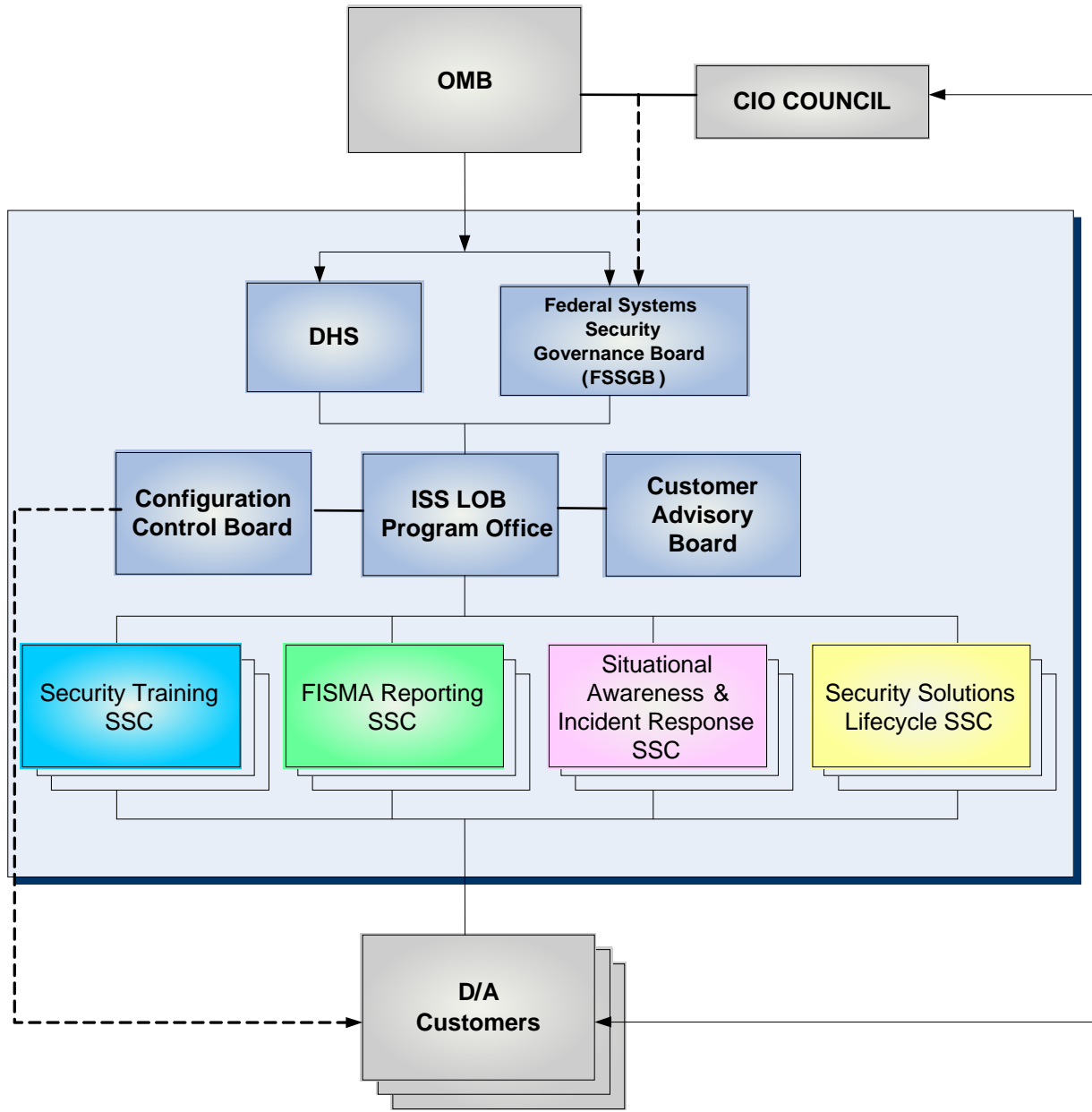
- Common Solutions in the following 4 areas:
  - Training
  - FISMA Reporting
  - Situational Awareness and Incident Response
  - Emerging Security Solutions for the Lifecycle
- Common Solutions close security gaps by establishing Share Service Centers (SSC) that:
  - drive better performance
  - increase expertise through specialization
  - reduction in cost by providing products and services common to civilian agencies, intelligence community, and DOD
- Governance Structure
- Phased Implementation

# Governance Structure

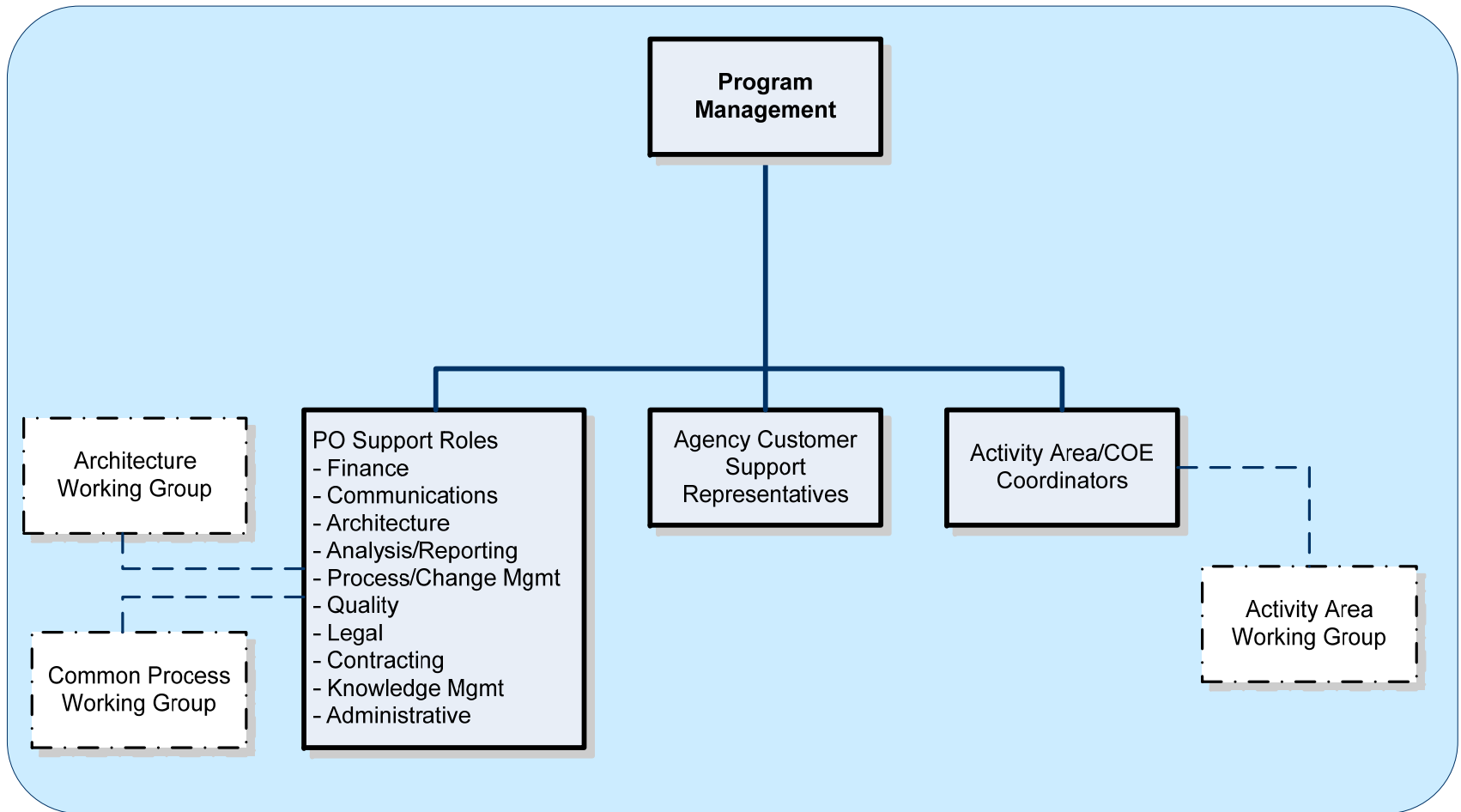
- ***Federal Systems Security Governance Board (FSSGB)*** - a multi-agency, multi-function oversight body and steering committee for the Information Systems Security Line of Business.
- ***Program Management Office (PMO)*** - established to facilitate the day-to-day operations of the ISS Line of Business based on guidance from the Board.
- ***Shared Service Centers (SSCs)*** - provide security products and services that are used by Customer agencies.
- ***Federal Agencies and Departments (Customers)*** – leverage common solutions provided by the SSCs to support their security requirements.



# Governance Structure



# Program Management Office



# High Level Implementation Schedule

		COE/Tier Phasing for ISS LOB (P = Plan/Manage, I=Implement/Acquire, Rm=Rollout Mandatory Tier, Ro=Rollout Optional Tier)																
Area	Specific Solutions/Activities	Timeframe																
		FY06		FY07		FY08		FY09		FY10		FY11		FY12		FY13		
		1H	2H	1H	2H	1H	2H	1H	2H	1H	2H	1H	2H	1H	2H	1H	2H	
FSSGB/PO	Plan/Manage ISS LOB	P	P	P	P	P	P	P	P	P	P	P	P	P				
Training COEs	Tier 1 - User Awareness Training		P	I	Rm	Rm	Rm											
	Tier 2 - Specialized Training (Optional)		P	I	I	Ro	Ro	Ro	Ro	Ro	Ro							
FISMA COEs	FISMA Reporting (Mandatory)		P	I	Rm	Rm	Rm	Rm	Rm	Rm								
SAIR COEs	Tier I – Core SAIR (Mandatory)		P	I	I	Rm	Rm	Rm	Rm	Rm	Rm							
	Tier II – Enhanced SAIR (Optional)			P	P	I	I	Ro	Ro	Ro	Ro	Ro	Ro					
	Tier III - Advanced SAIR (Optional)					P	P	I	I	Ro	Ro	Ro	Ro	Ro	Ro			
Security Solutions/ Life Cycle COEs	Tier I - Lifecycle (Mandatory)		P	P	I	I	Rm	Rm	Rm	Rm	Rm	Rm						
	Tier 2 - Advanced Lifecycle (Optional)			P	P	I	I	Ro	Ro	Ro	Ro	Ro	Ro					

(Once Planning/Management has begun for a COE, it continues throughout the life of the investment. Maintenance begins the year after implementation for a COE is completed.)

# Security Training

## Solution

- Common suites of ISS training products and training services for the Federal Government, to include government-wide licenses for commercial IT applications and security training products
  - User Awareness
  - Specialized Training

## Anticipated Outcomes

- Development of federal ISS skills standards & competencies to better align nationally recognized credentials to government ISS roles
- Infusion of ISS content into senior executive development & education programs
- Development of a repository of government sponsored/approved COTS training products and sources

# **FISMA Reporting**

## **Solution**

- Provide agencies with shared products & services to comply with FISMA reporting requirements - using pre-existing standardized tools for this process

## **Anticipated Outcomes**

- Government-wide process that can produce standardized FISMA results to OMB and lower FISMA processing costs
- Steady progress in terms of improving security maturity
- Automation allows for more efficient completion of the required annual security assessments and reporting, making it easy to keep information current to be used for program management - managers would also be in a better position to respond to ad hoc queries
- Improved program management capabilities would result in higher levels of compliance with performance standards - managers at all levels would be able to stay better informed and assure proper and timely action
- Efficiencies gained through use of central, standardized tools

# **Situational Awareness & Incident Response**

## **Solution**

- Multiple SSCs provide shared products and services for specific functional areas
- Provide federal enterprise situational awareness and incident response capability
- Start with functions providing a critical foundation for ISS, identifying others in future as Line of Business evolves

## **Anticipated Outcomes**

- Complements existing US-CERT/CIRT programs.
- Affordable alternative for smaller agencies to be served by larger agency to assist with information security without the huge cost to maintain the capability locally
- More uniform service approach, as the work will be mapped to a standard method for conducting the activity improving the consistency across government
- Aggregate requirements for tools and services, offering a choice of solutions to meet specific needs or proven practices
- Learn about experiences of other agencies with a particular product or service prior to making purchasing decisions
- Develop collection of common tools and practices that meet established standards, bringing consistency to the information systems security posture

# Emerging Security Solutions for the Lifecycle

## Solution

- Define a standardized 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 to be used by all agencies (to include risk management methodologies, cost benefit analyses, acquisition language, security planning tools)

## Anticipated Outcomes

- Standardized methodology will provide for interoperability of security solutions and services, repeatable implementation of product selection, providing non-repudiated means to ensure contractors and outsourcing providers follow the governments' mandatory baselines

# **SSC Responsibilities**

## **Establish SSC**

- Develop and execute detailed architecture and implementation plan for standing up SSC (SSC operational costs)
- Negotiate and acquire needed partnerships, tools, or other capabilities
- Implement/deliver Common Solutions
- Establish processes for operation/management of the SSCs
- Establish processes for communication, education and reporting to stakeholders; SSC Agency, ISS LOB, customers, other
- Develop and establish marketing materials and plan for signing up customer agencies
- Establish tracking and reporting process



# Considerations for Migrating Agencies

- Migrate over time to use of SSCs.
- Key considerations:
  - Service/products to migrate and associated migration schedules
  - Impacts to end users, management, business processes, and existing contractual obligations
  - Impacts to IT infrastructure (e.g., capacity, technology, communications, security and access controls, and help desk)
  - Data migration
  - Personnel transition
  - Asset disposition
  - Continuity of Operations
  - Change management
    - People
    - Process
    - Technology

# Customer Agencies Responsibilities

## **Customer D/A SSC Selection and Migration**

- Define agency requirements for the security area (What does the agency need?)
- Determine strategy for meeting requirements, e.g., migrate to SSC, adopt an agency, waiver to support internally, and migration timeframe SSL,
- Identify SSC exit or change strategy
- Develop and submit business case for strategy
- Develop Customer Agency criteria for selecting a SSC
- Evaluate and select SSC to provide common services for the Security Area
- Coordinate and execute IAA & SLA with SSC
- Migrate agency to SSC according to time period
- Perform change management to support the migration

# **Next Steps**

- **Coordinate SSC implementation/activities**
- **Coordinate/establish MOUs with SSCs**
- **Establish action plans for work groups**
- **Establish Security Solutions Work Groups**
- **Continue coordinate with FM/HR/IOI LOBs**

# Questions

Michael C. Smith  
Department of Homeland Security  
National Cyber Security Division  
mike.c.smith@dhs.gov