Information System Security Professional (ISSEPP)

A Practitioner’s View

Christopher Pohl
Booz Allen Hamilton
Linthicum, Maryland

Presentation for Annual Computer Security Applications Conference
December 11, 2003
Overview

- A Personal Perspective
- An Evolution in the Practice of Systems Security Engineering
- The ISSEP as an Integrated View of Information Assurance
- Improved Insight into Your Clients’ Challenges
- A Strategic View of Information Technology Management
- What is the ISSEP Return on Investment
A Personal Perspective

- 28 years as a law enforcement officer
  - Field, management, and policy level experience
  - Technology development – not just from a user perspective

- Private sector integration and consulting experience
  - Small business point of view
  - How technology can add value to service offerings

- Transition from government to public sector consulting
  - A different point of view than the traditional consultant
  - Insight into higher level drivers that affect security and technology issues

- Focus on the problem more than the solution
  - If you can properly frame the problem the solution is much easier
An Evolution in the Practice of System Security Engineering

The historical approach
- Now that we have built it, how do we secure it?
- Limited scope and scale of technology and security solutions
- Each system addressed separately
- An absence of collaborative view or common vision

The way ahead – the future of information assurance (IA)
- An integrated view of security objectives and features
- Baked in approach – implement security beginning with concept development
- Collaborative efforts with a common vision
- A more disciplined approach and view point
- Critical infrastructure assurance concerns
- Certification recognition
- International standards support, e.g., Common Criteria
The ISSEP as an Integrated View of Information Assurance

- Engineering ↔ Management
  - What—data, models, definitions
  - How—functions, processes, architectures, design
  - Who—organizations, people, timing

- Certification & Accreditation ↔ Policy Framework
  - Motivations—why, goals, strategies, objectives
  - Roles and responsibilities—the development and implementation process
  - Accountability—have we done it right and been good stewards?
Improved Insight into your Client’s Challenges

- Your clients’ challenges involve more than technology and security
  - Policy objectives and mandates
  - Federal information technology direction from Congress and OMB
  - Budget decisions are based on policy objectives not technology considerations
  - Clinger-Cohen Act
  - Federal Enterprise Architecture initiative
  - Other federal information security legislation
  - Privacy concerns

- Technology Portfolio Management
  - People—resources, human capital
  - Operations—what is the best and secure means to get the job done
  - Technology—tools that enable and enhance mission capabilities
A Strategic View of Systems and Security Engineering

- A holistic, life-cycle view of IA beginning with concept development
  - Protection—protective processes, methods, devices, etc.
  - Detection—the ability to sense abnormality indicating an attack, damage, unauthorized access or modification
  - Reaction/Response—actions to counter an attack and ensure safe and security recovery; continuity of operations

- Mastering the ISSEP Body of Knowledge
  - Alignment between policy and mission objectives
  - Better understanding of the need for integration and interoperability
  - Effective change management / transformation
  - Reduced “time to market” for your client
What is the ISSEP Return on Investment?

- Enhanced knowledge, skills, and understanding
  - Systems security engineering process
  - Why Certification and Accreditation is important
  - Technical Management
  - The role of policy direction and enforcement for federal agencies

- Greater professional opportunities
  - Employers and clients have more jobs than candidates with the right skill sets
  - You can effectively bridge the gap between policy, engineering, security and management disciplines

- Personal and professional satisfaction that your efforts are independently recognized
Questions?