Lessons Learned

A Craft Union/Trade School Approach to
Security Practitioner Training

James R Lindley
CSSLP, ISSEP, PMP, et al
16 March 2011
Background

• More than 50 years in electronics
• More than 30 years in computer programming
• Extensive experience in civil engineering, construction, and project management
• Approximately 30 years in electronic communications, intelligence analysis, and computer operations
• Currently the Senior Code Analyst and Technical Lead for the Penetration Testing and Code Analysis Team (PTCA) for a major federal agency
• **Craft unionism** refers to organizing … workers in a particular industry along the lines of the particular craft or trade that they work in by class or skill level. It contrasts with **industrial unionism**, in which all workers in the same industry are organized into the same union, regardless of differences in skill.
CSIS Report
A Human Capital Crisis in Cybersecurity
Technical Proficiency Matters

• There are continuing efforts by federal agencies to define an information technology (IT) security work force improvement program based on role definitions

• I contend: There is a lack of adequate detail in defining specialized IT security roles, especially as understood by managers without a security background or training.
Points to Ponder

• Simple evolves into Complex
• Complexity generates specialization
• Applications become APPLICATIONS
• Everybody wants to design, nobody wants to build
• Academia produces architects and engineers

• BUT…there is no degree in plumbing!
I am a dry pipe plumbing inspector.

- Static source code analysis (dry pipe)
- Penetration testing (wet pipe)
- Every stage of “plumbing” has a specialized creator and a specialized inspector
  - Requirements
  - Specification
  - Design
  - Code writing
  - Install and configure
  - Operations
  - Decommission
If You Build It Correctly, Security Will Come.

- If software security is an emergent quality, *from what* does software security emerge?

***The quality of all surrounding processes***

- Historically, most failed projects can trace their failure to the Requirements phase
FORGET DEVELOPER!!!!!!
Think Code-Writer

- Requirements Elicitor (Security policy)
- Specification Writer (Security Engineer)
- Application and Data Designers (Security Architects)
- Code Writers (Code Analysts, Pen Testers)
- Installation and Configuration (Pen Testers)
- Quality Assurance Testers (functional and non-functional)
- Operations and Operational Security (Security Monitors)
- Decommission (Data and application destruction specialists)

The Blue Collar Office Worker
How?

• Identify currently available skill sets in both federal and non-federal workers.
• Establish mentoring programs using what you already have available
• Find SPECIALIZED training (look to community colleges)
• Require contractual trainers to craft training IAW the agency policies
• GRANULATE your role definitions
Questions

- James.R.Lindley@IRS.GOV
- JamesLindley@Yahoo.com