Cyber Security Practitioner (CSP) Professionalization Program: 
An Approach for Professional Development -- 
Based on the Program Established at the Department of 
Veterans Affairs

Bruce Brody
ISPAB Meeting, September 2004
People – Key Building Block for Department-wide Security Program

1. In 2003, VA became the only large Department to centralize its cyber and information security functions at the Department level
2. OCIS currently has 118 FTE, ~$100+ million budget
3. OCIS is working to professionalize the 700+* VA cyber security practitioners in FY 2003
4. By 2004, a new Professionalization Directive and full certification of the information security work force will be completed, and VA will also boast one of the largest CISSP populations in Government

Goal: ISO (Information Security Officer) professionalization and certification will be the most comprehensive program of its kind in the Government

* This number includes full-time and part-time ISOs and alternate ISOs
Professionalization Overview

Finally, a promising practice for security personnel!

- Training ➔ VA Common Body of Knowledge; classroom training, Web-based module
- Testing ➔ 180 questions randomized off a list of 600 validated questions
- Certification ➔ Certifies that the individual is qualified to act as a VA Information Security Officer
- Ethics Statement ➔ An oath of acceptable behavior to which an ISO must adhere
- Background Investigation ➔ Confirmation that the individual can hold at least a Secret security clearance
- Credentialing ➔ Visible identification of an individual’s authority to act on behalf of OCIS
- Career Path/Incentives ➔ 2210 series PDs; career progression and mobility; monetary and non-monetary awards
- Re-Certification ➔ Post-certification training; re-testing; 3-year re-certification requirement
Principle 1

- Recognize that security is not a one-size fits all position
  - Position descriptions are needed to clearly identify roles and responsibilities of CSOs

**CSM**
manage the departmental cyber security program and provide policy, guidance, and oversight to the Administrations and Staff Offices

**ISO**
ensure operational compliance and effectiveness of security program elements that are not hardware or software related

**TSO**
ensure operational compliance and effectiveness of security program elements that are system (e.g., hardware/ software) related
Principle 2

- Training is a critical countermeasure and an essential element for all levels of the VA workforce:
  - CSPs must have a Department-wide focus and be able to bridge the differences between the operating administrations
  - Training must support development of general knowledge and skill, as well as industry certifications
  - VA’s Core Body of Knowledge (CBK) was developed from VA policy, NIST standards and guidelines, and industry best practices
    - Key domains of knowledge include: Security Fundamentals, Network Security, Security Controls, CSP Tasks, and Compliance
    - Major tasks: Risk Assessment, Security Plans, Certifications and Accreditation, Contingency Plans, Configuration Management, and Incident Response

Training...

- Remediates FISMA deficiencies and removes material weakness
- Develops work force competencies
- Communicates security requirements
- Enables a One-VA support structure
- Provides a standardized approach for improving performance
- Attains FITSAF levels 3 and above
Principle 3

- CSPs need a career path and a means to achieve vertical and horizontal growth:

Staff ISO
GS 7/9

Staff ISO
GS 11

Staff ISO
GS 12/13

Staff TSO
GS 12/13/14

Staff Team Lead
GS 13/14

TSO Supervisor
GS 13/14

ISO Team Lead
GS 13/14

ISO Supervisor
GS 13/14

TSO Team Lead
GS 13/14

TSO Supervisor
GS 13/14

CSM (Manager)
GS 14/15

Local facility or OCIS Regional Support Center or OCIS Central Office

OCIS Central Office

OCIS Regional Support Center
Principle 4

- Incentive programs are needed to reward, attract, and retain qualified CSPs
  - Pool of potential entry-level applicants is shrinking
  - The workforce is aging, and retirement eligible population is growing
  - Government jobs are viewed as relatively unattractive
  - Employee mobility is on the rise
  - Free agency approach to work is gaining popularity

Bottom Line: Competition for talent is keen

VA Incentive Options

- Compensation: advance payment for new hires, recruitment and relocation bonuses, retention allowances, superior qualification appointments
- Training: repay Federally-insured student loans (employee must sign 3-year service agreement); Homeland Security Act contained a provision that makes it easier for Agencies to cover the cost of employees' higher education
- Career development: opportunities for career advancement and organizational design
- Flexible work arrangements: telecommuting, job sharing, transit subsidy, time off for volunteer activities, Flexible Work Schedules (FWS), and Compressed Work Schedules (CWS)
Shifting Gears Slightly, What Are the Characteristics of a Professional Certification?

- **International** – based upon international compendium of industry “best practices” – (i.e., (ISC)²’s CBK®)
- **Examination** – Rigorous exam to assure knowledge of CBK
- **Independent** – Not product or service specific – Tests habitual knowledge
- **Endorsement** – Strict endorsement and audit process to verify candidate assertions
- **Ethics** – Comprehensive set of behavioral guidelines – Professional judgment
- **Experience** – Practical application of the CBK is acquired through experience
- **Re-certification** – Continuing education/training to maintain credential
- **Maturity** – Wide acceptance as the true measure of competency
(ISC)² Career Path – “Cradle-to-Grave Constituent Support”

Chief Information Security Officer

Chief Security Officer

Senior Security Engineer

Senior Network Security Engineer

Senior Security Systems Analyst

Senior Security Administrator

CISSP CONCENTRATIONS
- Pass Rigorous Specialty Exams: ISSAP, ISSER, ISSMP

CISSP
- Four Years Cumulative Experience
- Pass CISSP Exam
- Recertify Every Three Years
- Adhere to (ISC)² Code of Ethics

ASSOCIATE OF (ISC)²
- Pass CISSP Exam
- Adhere to (ISC)² Code of Ethics

Strategists’ Career Path

Continuous Training and Access to (ISC)² Resources

SSCP CONCENTRATIONS
- Credentials currently in development

SSCP
- One Year Cumulative Experience
- Pass SSCP Exam
- Recertify Every Three Years
- Adhere to (ISC)² Code of Ethics

ASSOCIATE OF (ISC)²
- Pass SSCP Exam
- Adhere to (ISC)² Code of Ethics

Tacticians’ Career Path
CISSP® ISO/IEC 17024 Accreditation – What it Means

• (ISC)² CISSP Credential
  – 1st worldwide information security credential to achieve ISO/IEC 17024
  – 1st IT organization to be accredited by ANSI for ISO/IEC 17024
• What does it mean for...
  – The information security profession
    • Global recognition and acceptance of CISSP
  – Businesses and governments
    • Discriminator for employers and businesses
  – (ISC)² CISSP credential holders
    • International recognition