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

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

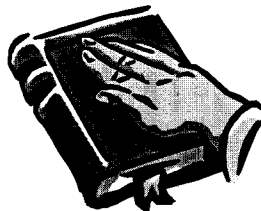


**VA Common Body of Knowledge;
classroom training, Web-based module**

Testing



**180 questions randomized off a list of
600 validated questions**



Certification

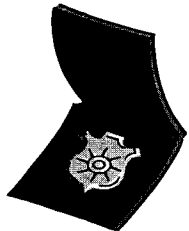


**Certifies that the individual is qualified to
act as a VA Information Security Officer**

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

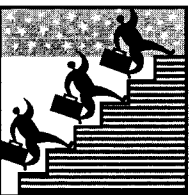


**2210 series PDs; career progression and
mobility; monetary and non-monetary awards**

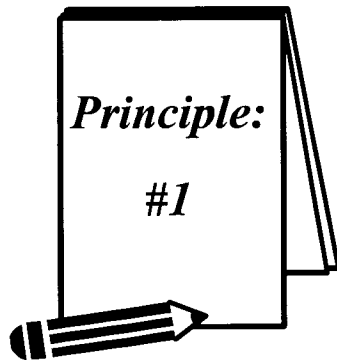
Re-Certification



**Post-certification training; re-testing; 3-year
re-certification requirement**

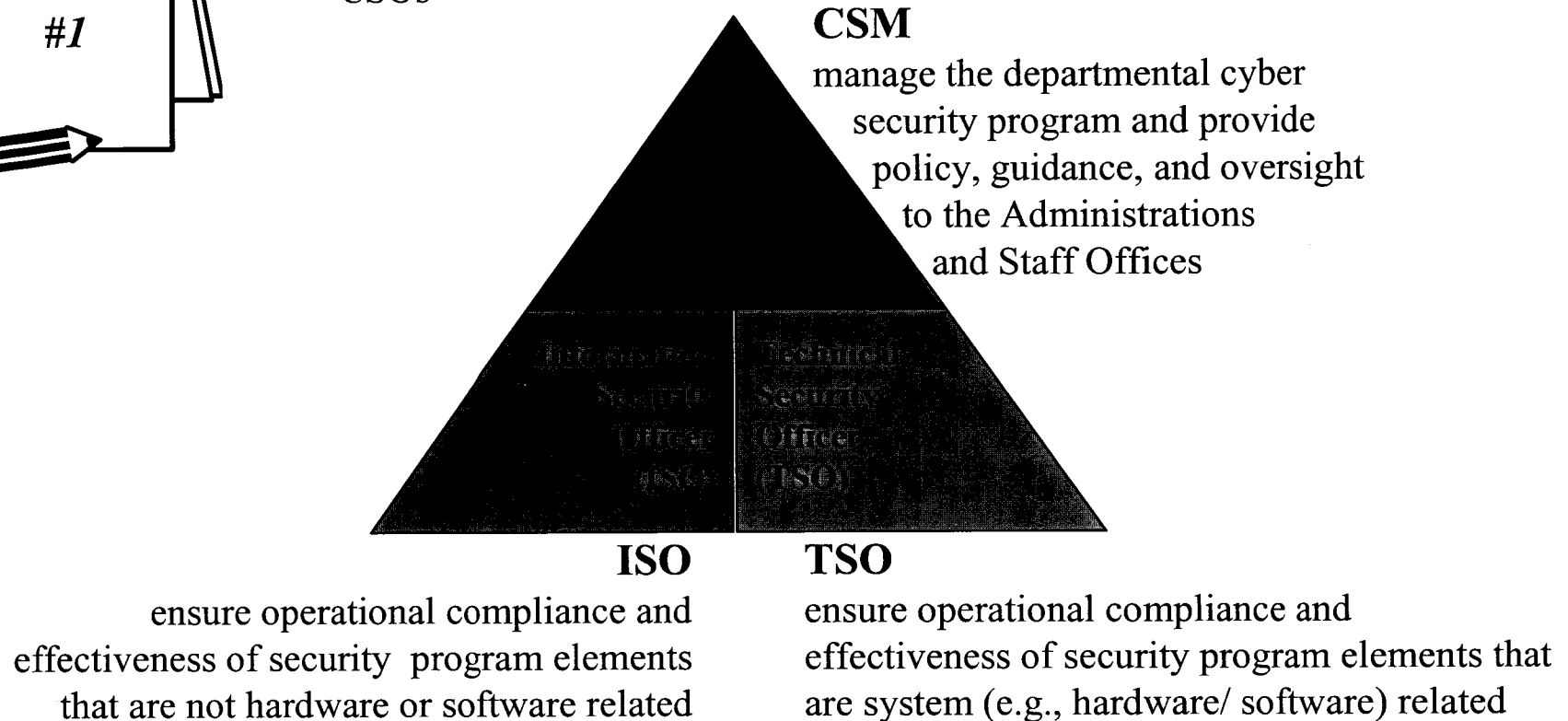


Principle 1

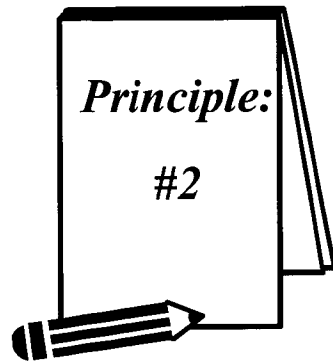


- **Recognize that security is not a one-size fits all position**

- Position descriptions are needed to clearly identify roles and responsibilities of CSOs



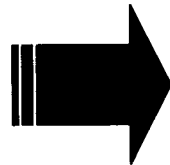
Principle 2



- **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...



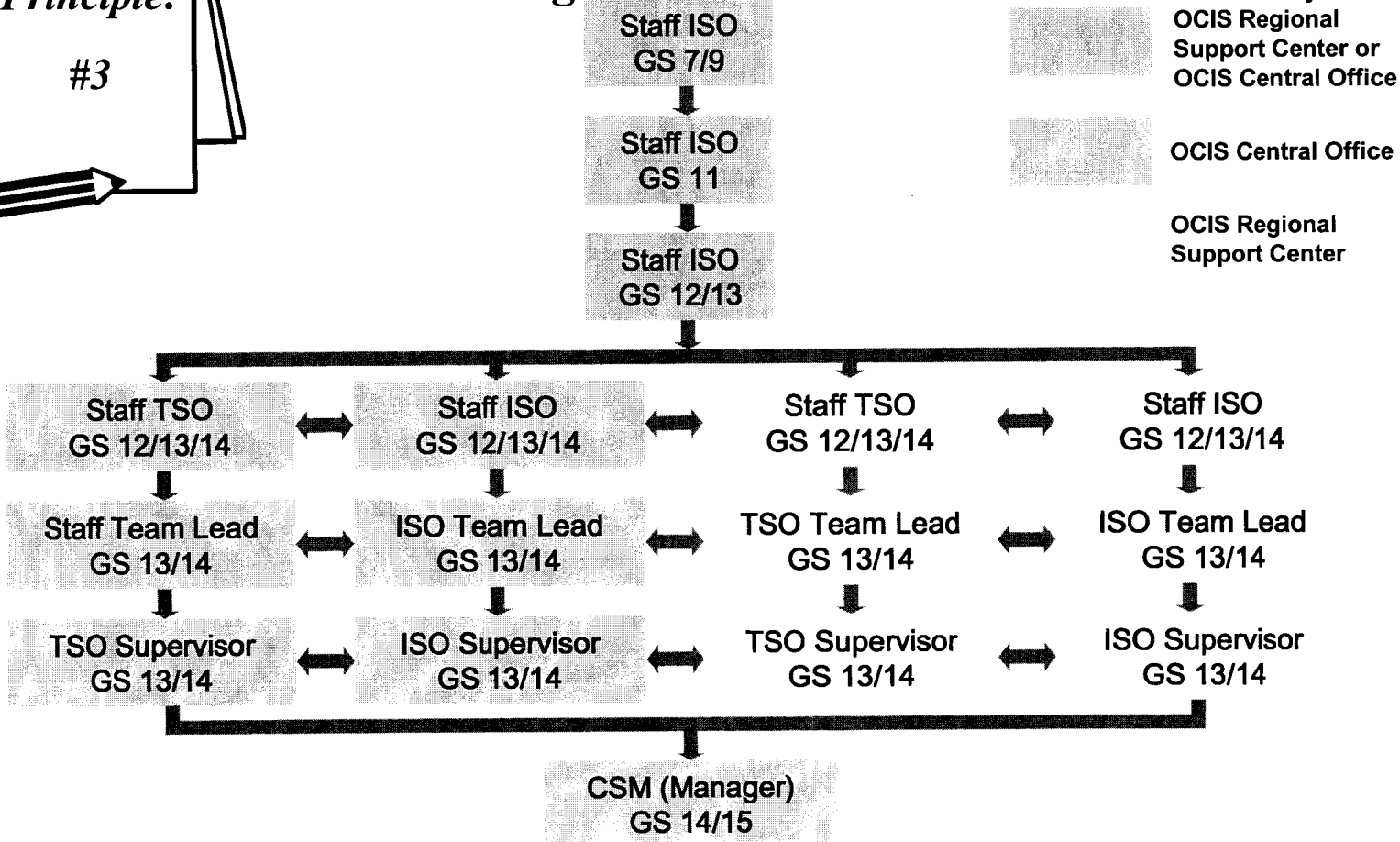
- Remediates FISMA deficiencies and removes material weakness
- Develops work force competencies
- Communicates security requirements
- Enables a One-VA support structure
- Provides a standardized approach for improving performance
- Attains FITSAF levels 3 and above

Principle 3

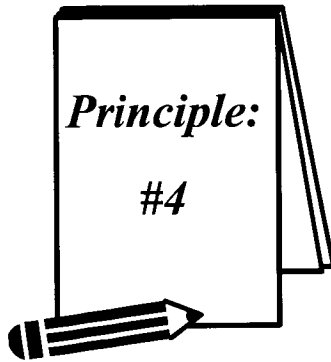
Principle:

#3

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



Principle 4

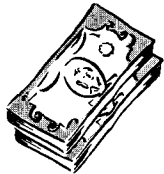


• Incentive programs are needed to reward, attract, and retain qualified CSPs

- 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

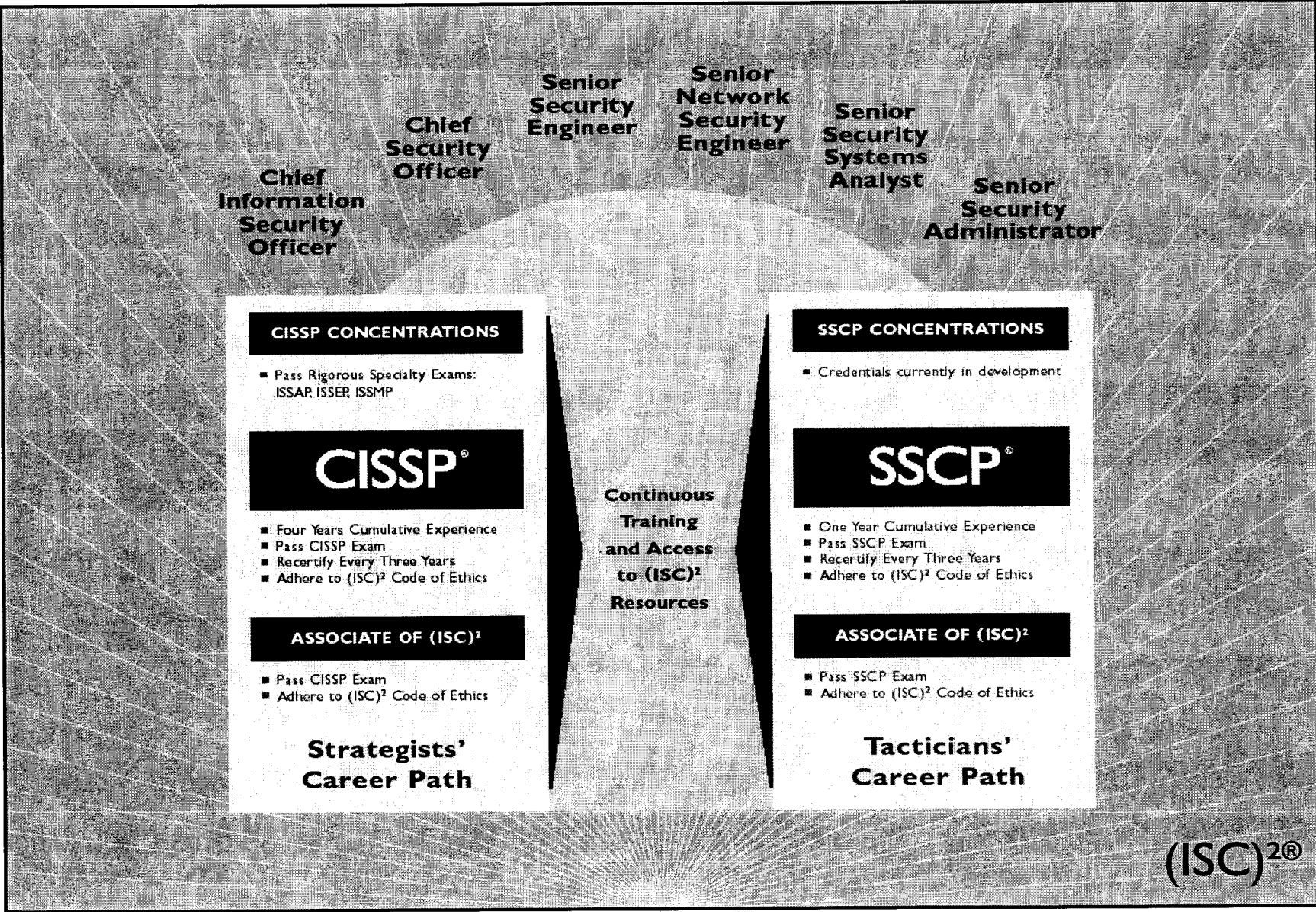


Flexible work arrangements- telecommuting, job sharing, transit subsidy, time off for volunteer activities, Flexible Work Schedules (FWS), and Compressed Work Schedules (CWS)

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”



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

