Lynn McNulty, CISSP
Information Security and Privacy
Advisory Board
November 2008
(ISC)^2 Overview & Background

- Global leaders in certifying and educating information security professionals with the CISSP® and related concentrations, CAP® and SSCP®.

- Established in 1989 – not-for-profit consortium of industry leaders.

- More than 60,000 certified professionals in over 135 countries.

- Board of Directors - top information security professionals worldwide.

- All of our credentials are accredited ANSI/ISO/IEC Standard 17024 and were the first technology-related credentials to receive this accreditation.
Did You Know?

• Over 70% of breaches of security vulnerabilities exist at the application level.*

* Gartner Group, 2005
Why Attack Applications?

- Attacking systems became harder
- Perimeter defenses improved
- Attacking applications became easier
- Application software became vulnerable and more exploitable
What is the Answer?

- No single answer
- Variety of solutions
- The following are addressing software development in a variety of ways:
  - **IEEE**: CSDA and CSDP (Software development)
  - **SANS**: GSSP-C, GSSP-J (Language specific/secure coding)
  - **ISSECO**: CSSE (Entry level education program with certificate of completion)
  - **DHS**: Software Assurance Initiative (Awareness Program/Forum)
  - **OWASP** – PCP (Web Application Development Security Certification)
  - **Vendor-Specific** (ex: Microsoft, Symantec) based on internal lifecycle processes/technology specific
- There is no indication that these organizations are addressing the content areas in the same manner as (ISC)².
The (ISC)² Approach – The CSSLP?

- Certified Secure Software Lifecycle Professional (CSSLP)
- Base credential
- Professional certification program
- Addresses security in the software lifecycle
- Takes a holistic approach to security in the software lifecycle
- Tests candidates competency (KSAs) to significantly mitigate the security concerns
Purpose

• The purpose of the Certification is to provide a credential that speaks to the individual’s ability to contribute to the delivery of secure software through the use of best practices.

• The target professionals for this Certification would be those who are involved in the Software Life Cycle activities.
Overview of (ISC)² Software Assurance Certification

Software Lifecycle Stakeholders

- Top Management
- Auditors
- Business Analysts
- Quality Assurance Managers
- Technical Architects
- Project Managers/Team Leads
- IT Manager
- Security Specialists
- Application Owners
- Developers/Coders
- Business Unit Heads
- Client Side PM
- Industry Group Delivery Heads

Secondary Target Influencers

- Application Owners
- Security Specialists
- Auditors

Primary Target Influencers

- Project Managers/Team Leads
- Technical Architects
- Business Analysts
- Quality Assurance Managers
- Business Unit Heads
- IT Manager
- Security Specialists
- Application Owners
- Developers/Coders
- Client Side PM
- Industry Group Delivery Heads

Influencers
- Secondary Target
- Primary Target
Market Drivers

• Has emerged as a global concern
• Off shoring of software development
• Minimize the potential for human error
• Software is not developed with security in mind
• Desire to meet growing industry needs
(ISC)² CSSLP CBK Domains

- Secure Software Concepts
- Secure Software Requirements
- Secure Software Design
- Secure Software Implementation/Coding
- Secure Software Testing
- Software Acceptance
- Software Deployment, Operations, Maintenance, and Disposal
CSSLP Certification Requirements

By Experience Assessment:
• Experience assessment will be open through 3/30/09
• Can be done on-line only
• Candidate will be required to submit:
  – Experience Assessment Application
  – Candidate agreement and agree to (ISC)² Code of Ethics
  – Detailed resume of experience
  – Four (4) essays detailing experience in four (4) of the following knowledge areas
    • Applying Security concepts to Software Development
    • Software Design
    • Software Implementation/Coding
    • Software Testing
    • Software Acceptance
    • Software Deployment, Operations, Maintenance, and Disposal
  – Fee of $650 with submission of applications
CSSLP Certification Requirements

By Examination:

- The first public exam will be held at the end of June 2009
- Candidate will be required to submit:
  - Completed examination registration form
  - Signed candidate agreement and agree to adhere to the (ISC)^2 Code of ethics
  - Proof of 4 years of FTE experience in the Software Development Lifecycle (SDLC) Process or 3 years experience plus a one year waiver of experience for 4 year degree or equivalent in an IT related field
  - Pay a Fee of $549 early-bird and $599 standard
- Candidate will be required to
  - Pass the official (ISC)^2 CSSLP certification examination
  - Complete the endorsement process
- The Associate of (ISC)^2 Program will apply to those who have passed the exam but will need to acquire the necessary minimum experience requirements
CSSLP Recertification Requirements

• Pay AMF’s annually ($100.00)
• Earn and submit a minimum of 15 CPE’s annually
• Earn and submit 90 CPE’s by the end of the 3-year certification cycle
• Adhere to the Code of Ethics
Future of CSSLP

- International Marketing Efforts
- ANSI/ISO/IEC 17024 accreditation
- Maintenance activities
- Cert Education Program
For more information, please contact:

- Tony Baratta, (ISC)$^2$ Director of Professional Programs
  - tbaratta@isc2.org

OR

- Vehbi Tasar, (ISC)$^2$ Manager of Professional Programs
  - vtasar@isc2.org