Security Certifications - 2016

Security Certifications

Roy Gertig, CISSP SSCP CISA CISM Security+ SCSecA
NSA-IAM/IEM PMP Project+ ITILv3 SSGB CVE4.0 TCC SCSA CIW-Pro Linux+ LPIC-1
SUSE-CLA Storage+ Server+ A+ N+ iNet+ CDIA+

Information current as of July 2016

SAIC
Redefining Ingenuity™

Disclaimer

- The acronyms used throughout this presentation are either ***"registered®"*** or ***"trademarked™"*** and are a product of their respective companies
- This presentation covers a multitude of certifications, but by no means is all inclusive
- This presentation is to be used as a resource and the links throughout work as of today

Agenda

- $(ISC)^2$ and Test Builds
- Government and Information Assurance
- Overview of Security Certifications
- Have some fun

First, a story

- Reminiscence

What do these have in common?

Redefining Ingenuity™

IRS / IG

SAIC Redefining Ingenuity™

Answer

We’re here to help!

What do these have in common?

Redefining Ingenuity™

(ISC)² / IRS

SAIC Redefining Ingenuity™

Answer

They both want your money!

(ISC)² Banquet

- Workshop Timetable
  - Starts on a Friday AM, ends Sunday PM
- NDA
  - 24 month limitation
  - Possible loss of CPE and Certs
- Why hold workshops
  - Several times a year to update and refresh item test bank

February AM

Why Security Certification?

Redefining Ingenuity™

Professional validation of skills

- Exposure to industry standards
- Understanding of best practices
- Demonstrate baseline skills for a specific role

Certification is not a substitute for years of experience

Certification, education, and experience together, can help make one a more well-rounded professional

SAIC Redefining Ingenuity™

Why Security Certification

Redefining Ingenuity™

Internal & external value

- Credible advice & support
- Quality of work & productivity
- Differentiation of your organization or group
- Culture of excellence

SAIC Redefining Ingenuity™

U.S. DoD Requirement – DoDD 8570.01

- Department of Defense Directive (DoDD) 8570.01 provided guidance and procedures for the training, certification, and management of all government employees who conduct Information Assurance functions in assigned duty positions (all personnel with "privileged (elevated) access" to DoD systems))
- These individuals are required to carry an approved certification for their particular job classification:
  - Any full or part-time military service member, contractor, or local nationals with privileged access to a DoD information system performing information assurance (security) functions – regardless of job or occupational series

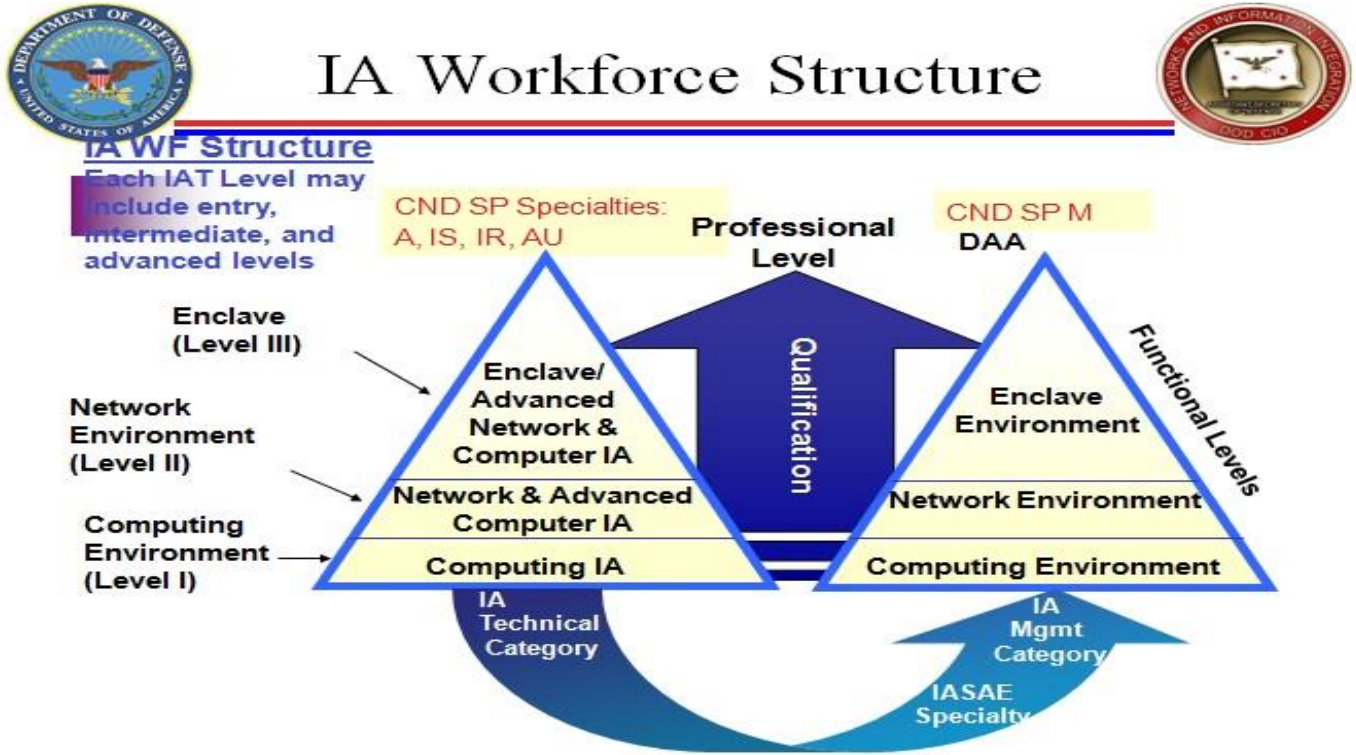
U.S. DoD Requirements - DoDD 8140.01

- DoDD 8140.01, dated 11 Aug 2015, Cyber Workforce Management replaced DoDD 8570.01 (as amended) effectively cancelling the document
- DoD Manual (DoDM) 8570.01-M Information Assurance Workforce Improvement Program (as amended on 11 Nov 2015) remains in effect.

- Unifies the overall cyberspace workforce and establishes specific workforce elements (cyberspace effects, cybersecurity, and cyberspace information technology (IT)) to align, manage and standardize cyberspace work roles, baseline qualifications, and training requirements. This directive does not address operational employment of the work roles. Operational employment of the cyberspace workforce will be determined by the Joint Staff, Combatant Commands, and other DoD Components to address mission requirements.

http://iase.disa.mil/iawip/Pages/policyref.aspx

DoD IA Workforce



http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf

DoD 8570 Certifications

Redefining Ingenuity™

Table AP3.T2 DoD Approved Baseline Certifications

IAT Level I	IAT Level II	IAT Level III
A+-CE Network+CE SSCP CCNA-Security	GSEC Security+CE SSCP CCNA-Security	CISA GCIH ~~GSE~~ GCED CISSP *(or Associate)* CASP CE
IAM Level I	**IAM Level II**	**IAM Level III**
CAP ~~GISF~~ GSLC Security+CE	CAP GSLC CISM CASP CE CISSP *(or Associate)*	GSLC CISM CISSP *(or Associate)*
IASAE I	***IASAE II***	***IASAE III***
CISSP *(or Associate)* CASP CE CSSLP	CISSP *(or Associate)* CASP CE CSSLP	CISSP - ISSEP CISSP - ISSAP

CNDSP Analyst	CNDSP Infrastructure Support	CNDSP Incident Responder	CNDSP Auditor	CNDSP Manager
GCIA CEH GCIH SCYBER	SSCP CEH	GCIH CSIH CEH GCFA SCYBER	CISA GSNA CEH	CISSP-ISSMP CISM

http://iase.disa.mil/eta/iawip/content_pages/iabaseline.html

SAIC Redefining Ingenuity™

Which certifications are right for me/my organization?

Redefining Ingenuity™

Organizational Needs Assessment:

- Roles & Responsibilities
- Experience
- Types of infrastructure computers, assets and equipment supported

SAIC Redefining Ingenuity™

DoD Workforce Certification (DWC)

- Cisco (Cisco)
- Computing Technology Industry Association (**CompTIA**)
- Information System Audit and Control Association **(ISACA)**
- International Information Systems Security Certification Consortium **(ISC)²**
- System Administration, Networking, and Security Institute **(SANS)**
- Carnegie Mellon Software Engineering Institute CERT **(SEI/CERT)**

Security Certifications – ISC²

Redefining Ingenuity™

CISSP- Certified Information Systems Security Professional

Common Body of Knowledge (2016)

- Security and Risk Management
- Asset Security
- Security Engineering
- Communications and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

SAIC Redefining Ingenuity™

Security Certifications – ISC^2

CISSP- Certified Information Systems Security Professional

Common Body of Knowledge (2009)

- Access Control Systems and Methodology
- Applications & Systems Development
- Business Continuity Planning
- Cryptography
- Law, Investigation & Ethics
- Operations Security
- Physical Security
- Security Architecture & Models
- Security Management Practices
- Telecommunications, Network & Internet Security

Security Certifications – ISC^2

CISSP Concentrations

- CISSP – ISSAP Architecture
- CISSP – ISSEP Engineering
- CISSP – ISSMP Management

Security Certifications – ISC^2

CISSP - ISSAP Architecture

- Access Control Systems and Methodology
- Communications and Network Security
- Cryptography
- Security Architecture Analysis
- Technology Related Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)
- Physical Security Considerations

Security Certifications – ISC^2

CISSP – ISSEP Engineering

- Systems Security Engineering
- Certification and Accreditation (C&A) / Risk Management Framework (RMF)
- Technical Management
- U.S. Government Information Assurance Related Policies and Issuances

Security Certifications – ISC^2

CISSP- ISSMP Management

- Security Leadership and Management
- Security Lifecycle Management
- Security Compliance Management
- Contingency Management
- Law, Ethics, and Incident Management

Security Certifications – ISC²

SSCP - Systems Security Certified Practitioner

Common Body of Knowledge (2016)

- Access Controls
- Security Operations and Administration
- Risk Identification, Monitoring, and Analysis
- Incident Response and Recovery
- Cryptography
- Networks and Communications Security
- Systems and Application Security

Security Certifications – ISC²

Redefining Ingenuity™

SSCP - Systems Security Certified Practitioner

Common Body of Knowledge (2009)

- Access Controls
- Administration
- Audit and Monitoring
- Risk, Response, and Recovery
- Cryptography
- Data Communications
- Malicious Code / Malware

SAIC Redefining Ingenuity™

Security Certifications – ISC²

Other ISC² Credentials

- CAP – Certified Authorization Professional
- CCFP – Certified Cyber Forensics Professional
- CCSP – Certified Cloud Security Professional
- CSSLP- Certified Secure Software Lifecycle Professional

Security Certifications – ISC²

Other ISC² Credentials

- HCISPP – HealthCare Information Security and Privacy Practitioner

Security Certifications – ISACA

– Certified Information Systems Auditor

Covers:

- The Process of Auditing Information Systems
- Governance and Management of IT
- Information Systems Acquisition, Development and Implementation
- Information Systems Operations, Maintenance and Service Management
- Protection of Information Assets

Security Certifications – ISACA

- Certified Information Systems Manager

Covers:

- Information Security Governance
- Information Risk Management and Compliance
- Information Security Program Development and Management
- Information Security Incident Management

Security Certifications – ISACA

- Certified in the Governance of Enterprise IT

Covers:

- Framework for the Governance of Enterprise IT
- Strategic Management
- Benefits Realization
- Risk Optimization
- Resource Optimization

Security Certifications – ISACA

- Certified in Risk and Information Systems Control

Covers:

- IT Risk Identification
- IT Risk Assessment
- Risk Response and Mitigation
- Risk and Control Monitoring and Reporting

Security Certifications – CompTIA

Redefining Ingenuity™

CompTIA Security+

- The exam covers system security, network infrastructure, cryptography, assessments, audits

CASP – CompTIA Advanced Security Practitioner

- Technical knowledge and skills required to conceptualize, design and engineer secure solutions across complex enterprise environments
- The CASP certification is intended to follow CompTIA Security+ or equivalent experience and has a technical, hands-on focus at the enterprise level.

SAIC Redefining Ingenuity™

Security Certifications – CompTIA

Redefining Ingenuity™

CompTIA A+

- The exams cover maintenance of PCs, mobile devices, laptops, operating systems and printers

CompTIA Network+

- The exam covers network technologies, installation and configuration, media and topologies, management, and security

SAIC Redefining Ingenuity™

Security Certifications - SANS

Redefining Ingenuity™

GIAC - Global Information Assurance Certification

29 certifications in: Security Administration, Forensics, Management and Software Security

SAIC Redefining Ingenuity™

Security Certifications – EC-Council

Redefining Ingenuity™

CEH - Certified Ethical Hacker

C|HFI - Certified Hacking Forensics Investigator

E|CSA - EC-Council Certified Security Analyst

LPT - Licensed Penetration Tester

SAIC Redefining Ingenuity™

Security Certifications – Offensive Security

Certified Professional

Wireless Professional

Certified Expert

Exploitation Expert

Web Expert

Security Certifications – ELearn Security

Security Certifications – CERT®

CSIH - Certified Computer Security Incident Handler

- Carnegie Mellon Software Engineering Institute – SEI /CERT Program
- For incident handling professionals, computer security incident response team (CSIRT) technical staff, system and network administrators with incident handling experience, incident handling trainers and educators, and individuals with some technical training who want to enter the incident handling field

Security Certifications – ASIS

Redefining Ingenuity™

CPP- Certified Protection Professional

- Demonstrated knowledge and experience in all areas of security management

PCI- Professional Certified Investigator

- Demonstrated education and/or experience in the fields of case management, evidence collection, and case presentation

PSP- Physical Security Professional

- Demonstrated experience in physical security assessment, application, design and integration of physical security systems, and implementation of physical security measures

SAIC Redefining Ingenuity™

Other Security Certifications

- American Society for Industrial Security (**ASIS**)
- International Information System Forensics Association (**IISFA**)
- Certified Wireless Network Professional (CWNP)
- Vendor or Product Specific

Security Certifications – IISFA

International Information Systems Forensics Association

CIFI - Certified Information Forensics Investigator

- Demonstrates expertise in all aspects of the information investigative process and is dedicated to bringing a level of consistency to the profession than can be recognized outside the field
- Domains of knowledge – Auditing, Incident Response, Law & Investigations, Tools & Techniques, Traceback and Countermeasures

Security Certifications – CWNP

Certified Wireless Network Professional

CWNA - Certified Wireless Network Administrator

- Radio Frequency (RF) Technologies
- IEEE 802.11 Regulations and Standards
- IEEE 802.11 Protocols and Devices
- IEEE 802.11 Network Implementation
- IEEE 802.11 Network Security
- IEEE 802.11 RF Site Surveying

CWSP - Certified Wireless Security Professional

- Wireless Network Attacks and Threat Assessment
- Security Policy
- Wireless LAN Security Design and Architecture
- Monitoring and Management

Security Certifications - Vendor

Vendor and Product Specific

- Hardware (ASIC) / Software dependent
- Range from intro to expert or advanced levels
- Examples include: Cisco, Check Point, Symantec, IBM, Oracle, Microsoft, and others

Security Certifications - Vendor

- Cisco:
  - CCNA Security
  - CCNP Security
  - CCIE Security
  - SCYBER
- Check Point:
  - Check Point Certified Security Administrator (CCSA)
  - Check Point Certified Security Expert (CCSE)
  - Check Point Managed Security Expert (CCMSE)
  - Check Point Certified Security Master (CCSM)
- Microsoft
  - Microsoft Certified Systems Engineer (MCSE)
  - Microsoft Certified Systems Administrator (MCSA)

Other Certifications

IAPP - International Association of Privacy Professionals

- CIPP - Certified Information Privacy Professional (C/E/G/US)
  - Demonstrates understanding of privacy and data protection practices in the development, engineering, deployment and auditing of IT products and services
- CIPM – Certified Information Privacy Manager
  - Privacy program governance and the skills to establish, maintain and manage a privacy program across all stages of its operational life cycle
  - The CIPM complements the CIPP designation by demonstrating that in addition to understanding laws and regulations around privacy, you also understand how to operationalize privacy in your organization through process and technology
- CIPT – Certified Information Privacy Technologist

Certified Information Privacy Professional (CIPP)

Other Certifications

PMI - Project Management Institute

Below are four of eight certifications that PMI offers:

- CAPM – Certified Associate Project Management
- PMI – RMP– PMI Risk Management Professional
- PMP – Project Management Professional
- PgMP – Program Management Professional

ACFE – Association of Certified Fraud Examiners

- CFE– Certified Fraud Examiner

2016 Hot Certifications

Redefining Ingenuity™

Citrix Certified Enterprise Engineer for Virtualization
CompTIA Security+
GIAC Certified Windows Security Administrator
Certified Computer Examiner
AWS Certified SysOps Administrator-Associate (Cloud)
EC-Council Certified Security Analyst
Mongo DB Certified DBA
Microsoft Certified Solution Developer: Applications Lifecycle Management
Cisco Certified Design Associate
Certified in the Governance of Enterprise IT

http://www.cio.com/article/2891552/careers-staffing/it-certification-hot-list-2015-10-that-deliver-higher-pay.html#slide1

SAIC Redefining Ingenuity™

2016 Hot Certifications (cont'd)

Redefining Ingenuity™

AWS Certified Solutions Architect – Associate
Certified in Risk and Information Systems Control (CRISC)
Certified Information Security Manager (CISM)
Certified Information Systems Security Professional (CISSP)
Project Management Professional (PMP)
Certified Information Systems Auditor (CISA)
Cisco Certified Internetwork Expert (CCIE) Routing and Switching
Cisco Certified Network Associate (CCNA) Data Center
Cisco Certified Design Professional (CCDP)
Certified Ethical Hacker (CEH)
Six Sigma Green Belt
Citrix Certified Professional - Virtualization (CCP-V)
Cisco Certified Networking Professional (CCNP) Security
ITILv3 Foundation
VMware Certified Professional 5 - Data Center Virtualization (VCP5-DCV)
https://www.globalknowledge.com/us-en/content/articles/top-paying-certifications/

SAIC Redefining Ingenuity™

Security Certifications – Best for 2016

- CompTIA Security +
- CEH: Certified Ethical Hacker
- GSEC: SANS GIAC Security Essentials
- CISSP: Certified Information Systems Security Professional
- CISM: Certified Information Security Manager

Toms IT Pro

References & Resources

- ICS^2 - International Information Systems Security Certifications Consortium, Inc. https://www.isc2.org
- ISACA - Information Systems Audit and Control Association, https://www.isaca.org/
- SANS - SysAdmin, Audit, Networking and Security Institute, https://www.sans.org/
- GIAC - Global Information Assurance Certification, https://www.giac.org/
- IAPP - International Association of Privacy Professionals, https://www.privacyassociation.org/
- CompTIA - IT Industry Association, https://www.comptia.org/home.aspx
- EC-Council - https://www.eccouncil.org/
- Carnegie Mellon University Software Engineering Institute, CERT
  - http://www.sei.cmu.edu/training/certificates/security/index.cfm
  - http://www.sei.cmu.edu/certification/opportunities/index.cfm
- ASIS - American Society for Industrial Security, https://www.asisonline.org/Pages/default.aspx
- IISFA - International Information Systems Forensics Association, http://www.iisfa.net/
- PMI – Project Management Institute, http://www.pmi.org/
- CWNP – Certified Wireless Network Professional, http://www.cwnp.com/

References & Resources

- Department of Defense, DoD 8570.01-M
  http://iase.disa.mil/eta/iawip/content_pages/iabaseline.html
- What are U.S. DoD 8140, 8570, and 8570-01-M and What do they mean for Your Career?
  - CompTIA Article on DoD 8140/8570/8570-01-M (11 Sep 15)
- Certification Magazine – http://certmag.com
  - Roy Gertig Certmag Interview (2003) - http://certmag.com/changing-your-tune-to-technology/
- CCCure – http://www.cccure.org/
- Offensive Security - https://www.offensive-security.com/
- Elearn Security - https://www.elearnsecurity.com/
- IA Workforce Certification Providers
  http://iase.disa.mil/iawip/Lists/IA%20Workforce%20Certification%20Providers/AllItems.aspx
- National Initiative for Cybersecurity Education (NICE) - http://csrc.nist.gov/nice/workforce.html

Certification Matrix

ISC²	CISSP	SSCP	CAP	CSSLP	CCFP	HCISPP	CCSP	
ISACA	CISA	CISM	CGEIT	CRISC				
SANS/GIAC	GSEC GWAPT GISF GCUX GLEG	GCIH GCFE GCED GSSP-JAVA GMON	GCIA GREM GISP GMOB GSSP-.NET	GCFA GSNA GICSP GNFA GCPM	GPEN GPPA GAWN GCCC GPYC	GSLC GCWN GXPN GWEB GASF		
EC-COUNCIL	CEH	C|HFI	E|CSA	LPT				
Comp-TIA	CASP	Security+	Network+	A+				
CWNP	CWTS	CWNA	CWSP	CWDP	CWAP	CWNE	CWNT	

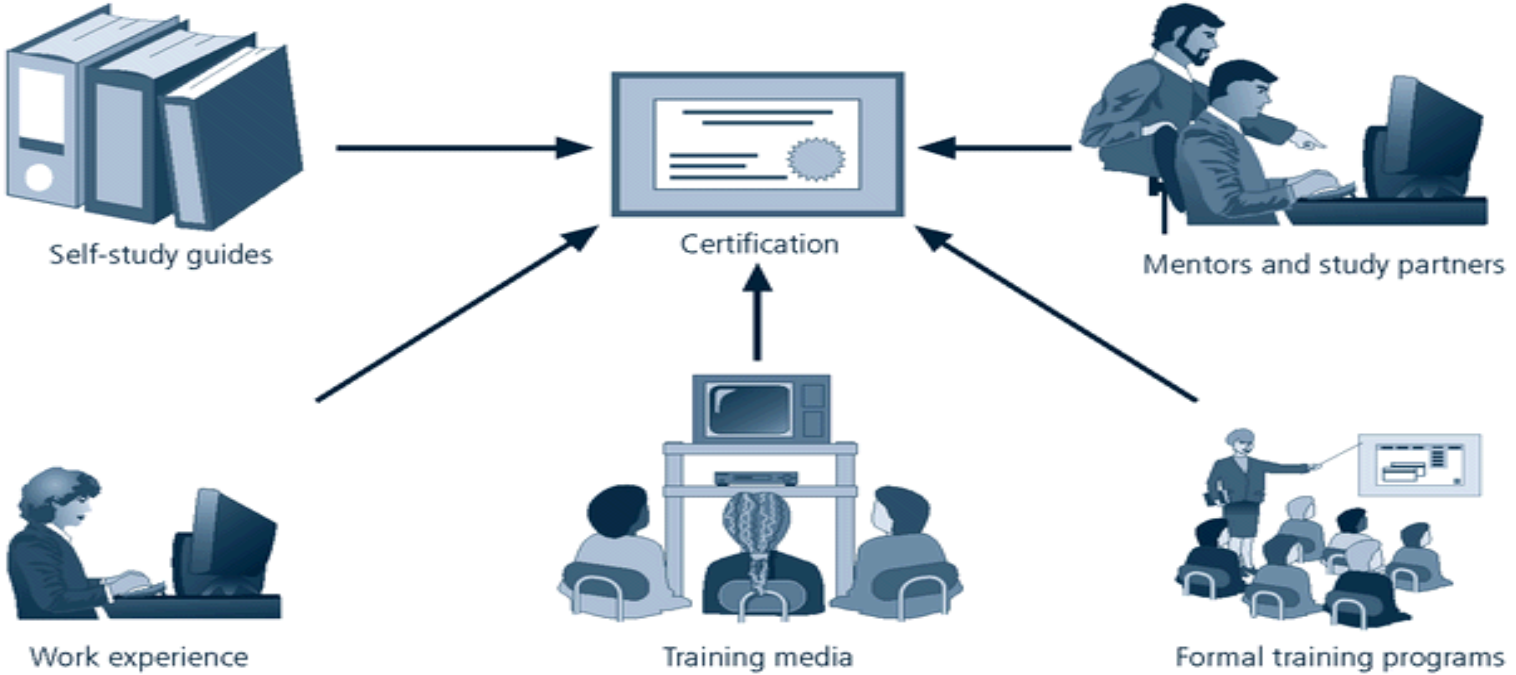
Certification Matrix (cont'd)

Redefining Ingenuity™

SEI/CERT	CSIH							
ASIS	CPP	PCI	PSP					
IAPP	CIPP	CIPM	CIPT					
IISFA	CIFI							
ACFE	CFE							
PMI	PMI-RMP	PMP	PgMP					
Cisco	CCNA Security	CCNP Security	CCIE Security	SCYBER				
Offensive-Security	OSCP	OSWP	OSCE	OSEE	OSWE			
Elearn Security	eCPPT	eCRE	eJPT	eMAPT	eNDP	eWDP	eWPT	eWPTX

SAIC Redefining Ingenuity™

Preparing for Security Certification



Maintaining Certifications

Almost all certifications require some form of continuing education to maintain the certificate:

- ISC² & ISACA require 120 hours of Continuing Professional Education (CPE) credits over 3 years. At least 40 CPEs must be earned annually for CISSP, 20 CPEs for ISACA certs.
- PMI requires 60 Professional Development Unit (PDU) credits over 3 years.

Questions?

Security Certifications - 2016