DIA's DoD 8570.01-M
FISSEA 2008 Annual Conference

Mr. Paul Krasley

11-13 March 2008

Outline

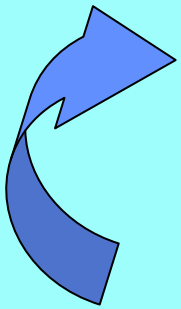
- **You said “Free”**
  - Inventory your Staff
  - Pick your Certifications
  - Tell your Vendors
- **DoD Provided Resources**
  - Carnegie Mellon Univ
  - SANS
  - ISACA
  - COMPTIA
  - Vouchers
  - Maintenance Fees
- **Training Available**
  - University of Fairfax
  - Tuition Reimbursement
- **DIA Training Team**
  - SME’s
  - Schedule
  - Resources
  - CPE’s
- **Issues**
  - DFARS
  - FISMA

Overview

- It takes no money to re-evaluate your staff who currently have the “keys to the kingdom” and re-assign and or remove privileged access to increase your organizational security and information assurance risk.

- Reducing the number of privileged users and centralizing the IA support with a reduced, better trained and certified IA staff is goal.

You said “Free”



- Inventory your Staff
  - Re-assign Embedded (0-14) & Additional (15-25)
  - Start hiring certified staff now
  - DIA as an example
- Pick your Certs
  - Current Certifications
  - Security + and CISSP
    - T-II & III, M-I, II, & III
    - Carnegie Mellon University CERT
- Tell Your Vendors

DoD Provided Resources

- Carnegie Mellon
  - Security + and CISSP paid for by DoD
- SANS
  - GISF, GSEC, GSLC, GISP (CISSP)
  - GCIA & GCIH (CND)
- ISACA: CISA & CISM
- COMPTIA: A+, Network +, & Security +
- Vouchers
- Maintenance Fees

Training Available

- Univ. of Fairfax (Dr. Victor Berlin: vberlin@ufairfax.net)
  - Free to all
- Use Tuition Reimbursement
  - Global Knowledge http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=8029&country=United+States
  - Training Camp http://www.trainingcamp.com/usa/training/isc2/cissp/overview.aspx
  - Kaplan University http://www.getinfo.kaplan.edu/Microsite_B/InformationTechnologyinforeq.aspx?ID=5&HAC=0
  - InfoSec Institute http://www.infosecinstitute.com/courses/cissp_bootcamp_training.html

DIA Training Team

Directorate for Information Management & CIO

- 16 CISSP
- 1 ISSEP
- 1 CISM
- 5 A+
- 1 Network +
- 1 GSLC
- 2 GSEC
- 19 IASE

Mailbox: IATraining@dia.ic.gov
cnkrapf@dia.ic.gov
paul.krasley@dia.mil

Civilian and Military as Certification SME

Training Group Mentors

Questions and Answers

Technical Security and IA SME's

IA Training Schedule

• Jan, Feb, Mar	Test	April
• Feb, Mar, April	Test	May
• Mar, April, May	Test	June
• April, May, June	Test	July
• May, June, July	Test	August
• June, July, August	Test	Sept
• July, August, Sept	Test	Oct
• August, Sept, Oct	Test	Nov

IA Training Resources

- DIA selected DISA CBT sections
- OPSEC and Identity Theft on-line or CBT
- New DISA Security Shorts is outstanding. http://iase.disa.mil/index2.html.
- CyberCiege from the Navy. http://cisr.nps.edu/cyberciege
- Reference Manuals as possible
  - ISC2 only for SSCP and CISSP
  - ISACA Local Chapters for CISA & CISM
  - COMPTIA multiple vendors

DoDIIS Enterprise CPE's & Professional Development

DoDIIS Enterprise (all users)

- DoD IA Awareness (1.5)
- Basic SCI System User (3)
- Information Security Shorts (Insider Threat, Passwords, SCADA, Identity Theft (1))
- IAP&T – Overview (.75)

IAO, Privileged User

- STIG Auditing Logs (.25)
- Windows 2000 Security (10)
- Firewalls & Routers (3.5) *
- IAP&T (4)
- DCID 6/3 (6)
- SAPIR UNIX (8)
- UNIX Security for SA (40)
- WEB Security (6)
- Database Security (1.5)
- Hardening the DoDIIS Enterprise: Hands-On (10) – (IAO only)
- DoDIIS System Compliance Registry (DSCR) (4) - (IAO only)

IAM, RIAM, ISSE, Certifier

- DoD Certifier Fundamentals (8)
- Retina & REM (10)
- DAA (3)
- SSAA (1.5)
- Hardening the DoDIIS Enterprise: Hands-On (10)
- DoDIIS System Compliance Registry (DSCR) (4)

CIAO, DCIAO, RCIAO, SCO

- Cyber Law, Cyber Space (2)
- Active Defense (1)

Issues: DFARS

Information Assurance Contractor Training and Certification — DFARS Case 2006-D023

Procedures, Guidance, and Information

PGI 239—ACQUISITION OF INFORMATION TECHNOLOGY

[PGI 239.71--SECURITY AND PRIVACY FOR COMPUTER SYSTEMS

PGI 239.7102 Policy and responsibilities.

PGI 239.7102-3 Information assurance contractor training and certification.

(1) The designated contracting officer's representative **will document** the current information assurance **certification status of contractor personnel** by category and level, in the Defense Eligibility Enrollment Reporting System, as required by DoD Manual 8570.01-M, Information Assurance Workforce Improvement Program.

(2) DoD 8570.01-M, paragraphs C3.2.4.8.1 and C4.2.3.7.1, **requires modification of existing contracts** to specify contractor training and certification requirements, in accordance with the phased implementation plan in Chapter 9 of DoD 8570.01-M. As with all modifications, any change to contract requirements shall be with appropriate consideration.]

Issues: FISMA Reporting

Table 1: IA Workforce Primary Duty Positions
Table 2: IA Workforce Additional or Embedded
Table 3: IA Workforce Certification / Recertification

Table 1: IA Workforce Primary Duty Positions

	Civilian			Military			Contractor	
	Number	Filled	Certified	Number	Filled	Certified	Filled	Certified
IAT I								
IAT II								
IAT III								
IAM I								
IAM II								
IAM III								
CND-A								
CND- IS								
CND-IR								
CND-AC								
CND-SPM								
IASE I								
IASE II								
IASE III								
Total								

"Against 8570"

- I have a degree; I don't need a certification
- I've been doing the job for 15 years, I don't need a certification
- The value of a certification is weakened by a high number of certified people
- I know lots of people who passed the [certification] test but can't do the job
- I've been trying to get money for 5 years to get my folks training; I finally got it after I showed my boss the 8570 manual
- If I get my people certified they'll quit and become contractors
- 8570 is not in place to help you **do** your mission, it is in place to make you change **how** you do your mission

Questions

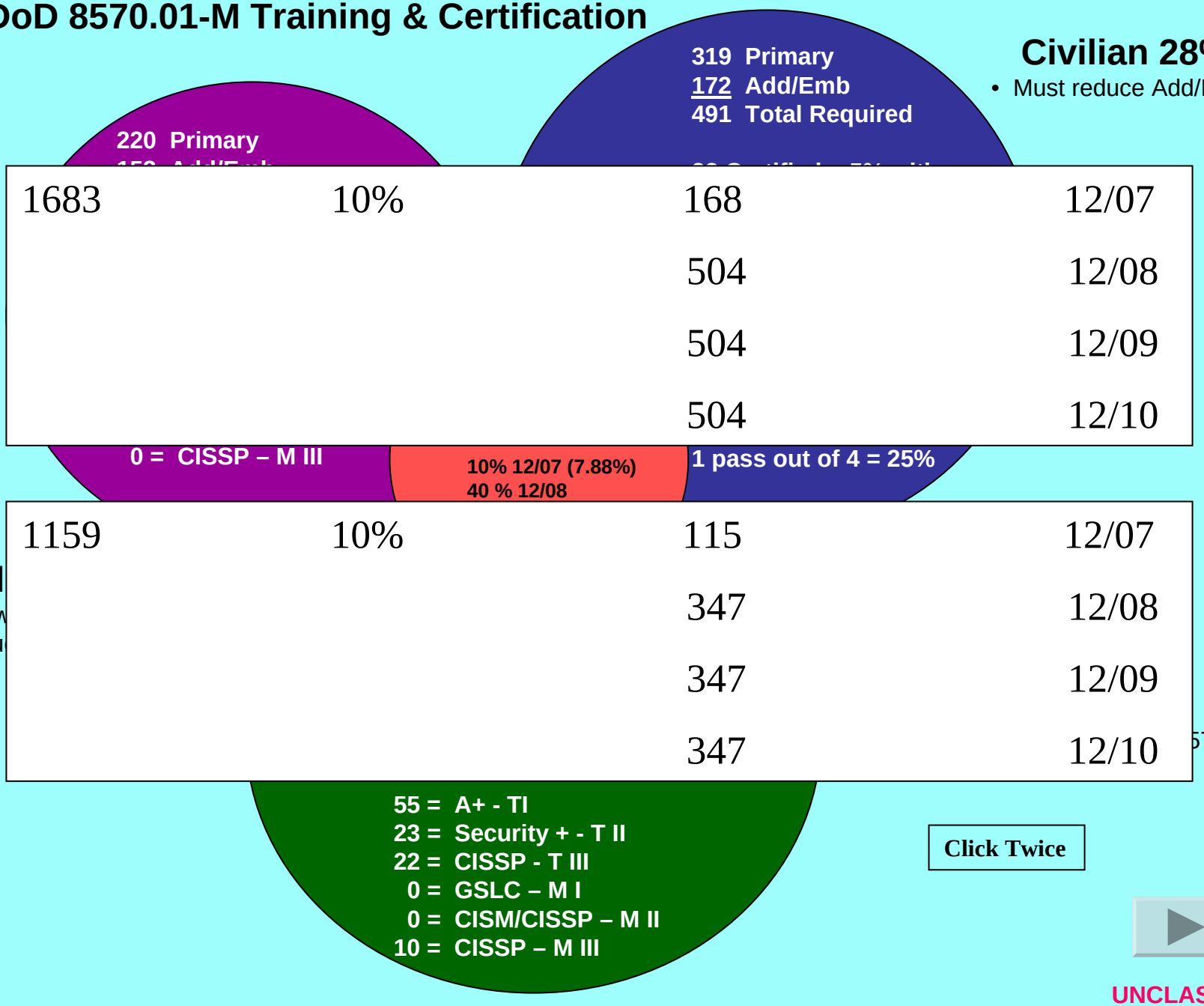
Directorate for Information Management & CIO

Paul Krasley, IA Training

202-231-2387

paul.krasley@dia.mil

DIA DoD 8570.01-M Training & Certification



Civilian 28%

- Must reduce Add/Emb

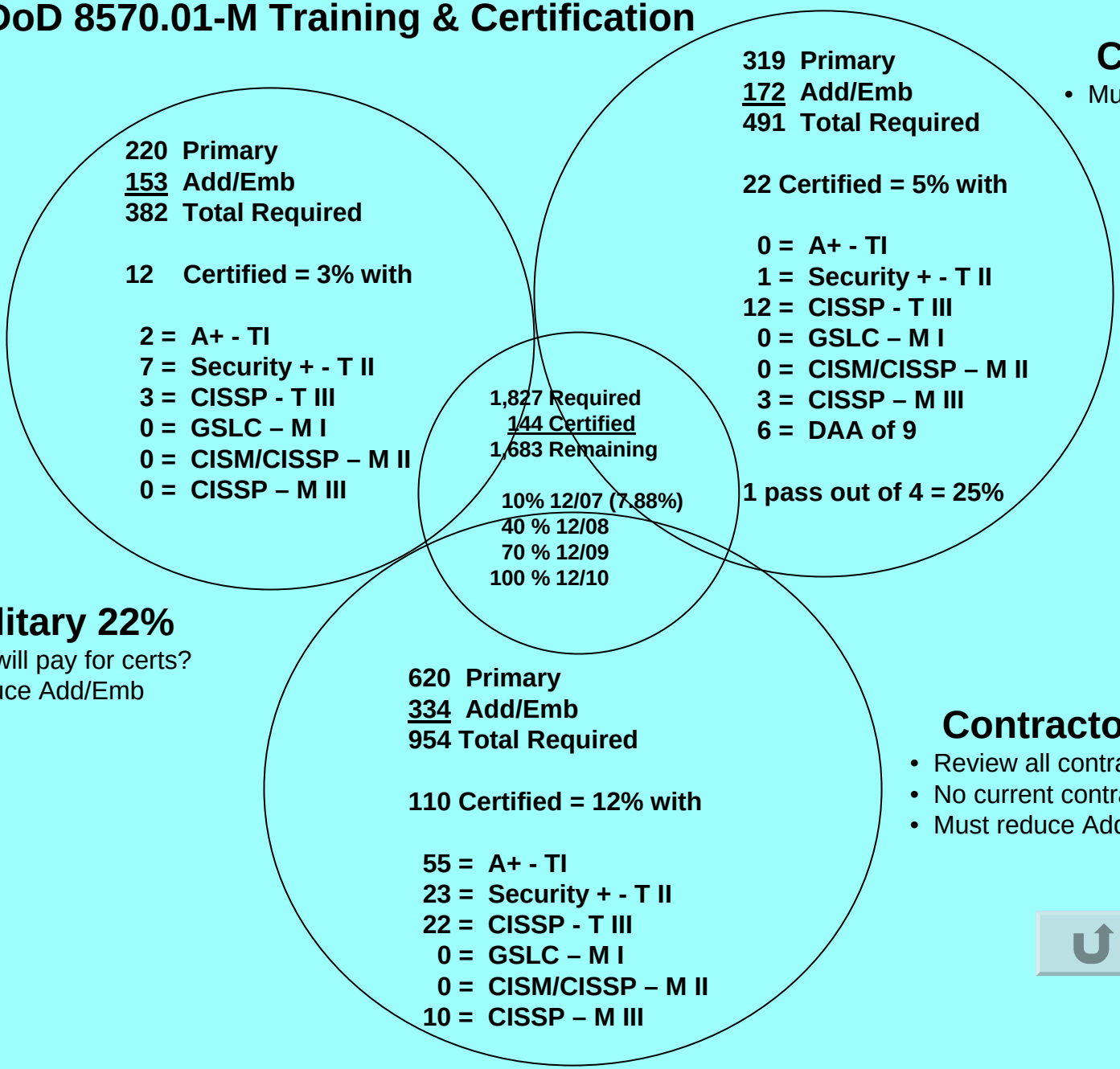
Mil

- DIA w
- Redu

570

Click Twice

DIA DoD 8570.01-M Training & Certification



Civilian 28%

- Must reduce Add/Emb

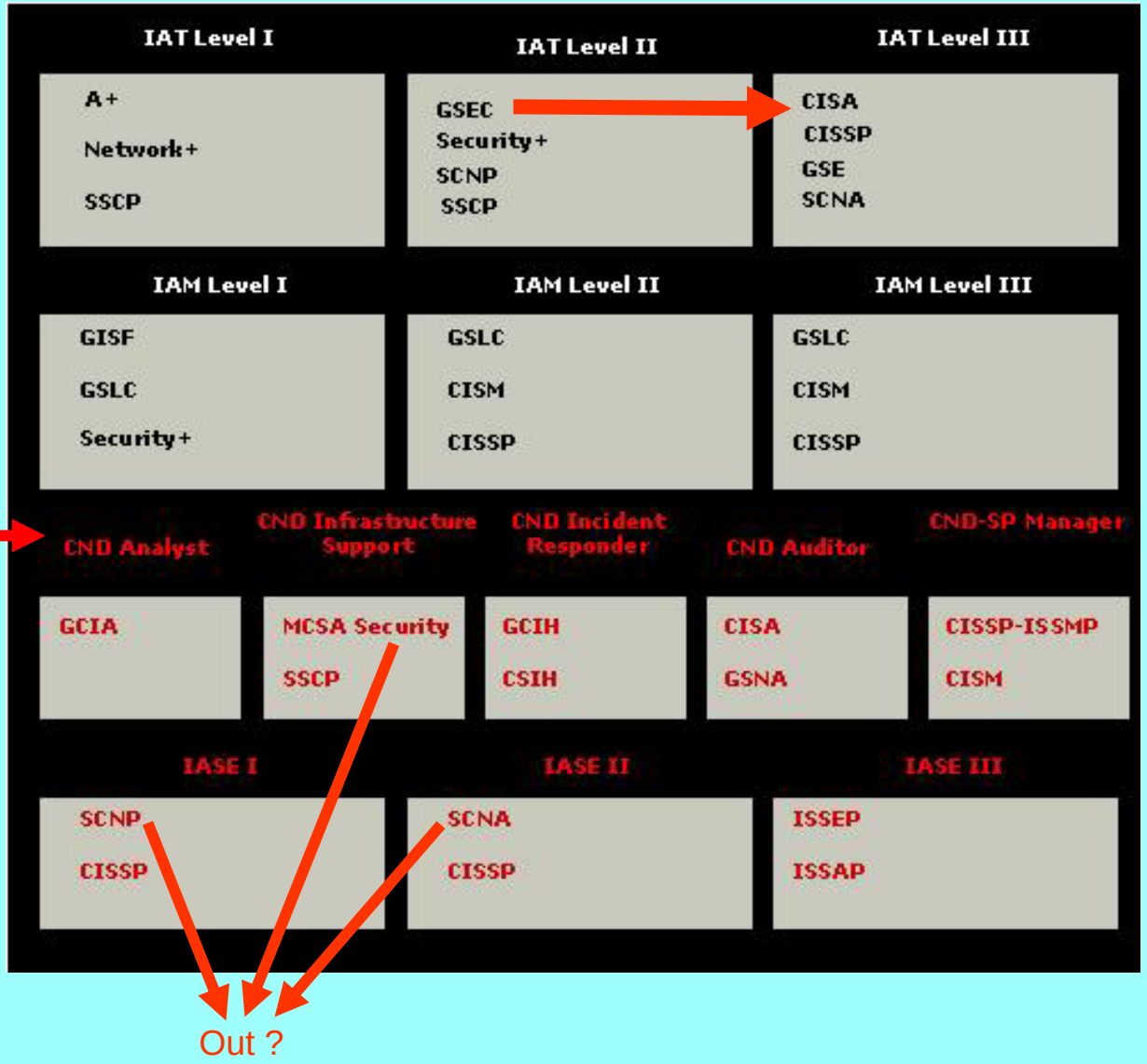
Military 22%

- DIA will pay for certs?
- Reduce Add/Emb

Contractors 50%

- Review all contracts
- No current contracts include 8570
- Must reduce Add/Emb

Current Proposed Certifications Under Review



https://www.vte.cert.org/VTEWEB/default.aspx

Jump To: CERT | Software Engineering Institute | Carnegie Mellon University Browser Check | Log

CERT | Virtual Training Environment

Home | Library | Training | About VTE | Get Access | Hel

The CERT **Virtual Training Environment** (VTE) - A revolutionary resource for information assurance, incident response and computer forensic training, with over 500 hours of material available. VTE blends the best of classroom instruction and self-paced online training, delivering training courses, anytime access to answers, and hands-on training labs all through a standard Web browser.
VTE is produced by the CERT® program of the Software Engineering Institute at Carnegie Mellon University.

Some of the VTE material is available for FREE in the VTE Public Library. Access to the VTE training courses and hands-on training labs requires an account.

Members or affiliates of some organizations are eligible for accounts under sponsorship agreements. Current VTE Access programs:

- Members of the DoD may request free VTE accounts under a sponsorship agreement with DISA for DoD D 8570.1 compliance training. Review eligibility requirements and program benefits or request an account now.
- Premium Access trial account. Anyone with an interest in Information security may request a trial account to VTE Premium Access with hands-on labs. Accounts are valid for 14 days and include access to the entire premium content library. Request an account now, or learn more about how to obtain full subscriptions to the material.

Not covered by a sponsorship agreement? You can still use the free VTE Public Library, learn more about VTE, then sign up for a trial account.

Interested in learning more? Follow the instructions below.

James Wrubel
VTE Team Lead
CERT
jcw@cert.org
+1 412 268 3182
https://www.vte.cert.org

Current & Users

First make sure your computer is set up for VTE, then log in to begin training:

- Access your current courses
- Log in to access VTE Library Premium Content
- VTE readiness Browser Check

Organizations

Learn more about VTE and how it can help you support skill development and compliance training initiatives in information security, computer forensics, and incident response:

- See the materials in the VTE Public Library and decide if they are useful to your organization
- Request a trial account for VTE Premium Access to experience hands-on labs for yourself.
- Review VTE public and private courses
- Contact CERT to develop a training and skill development program for your organization

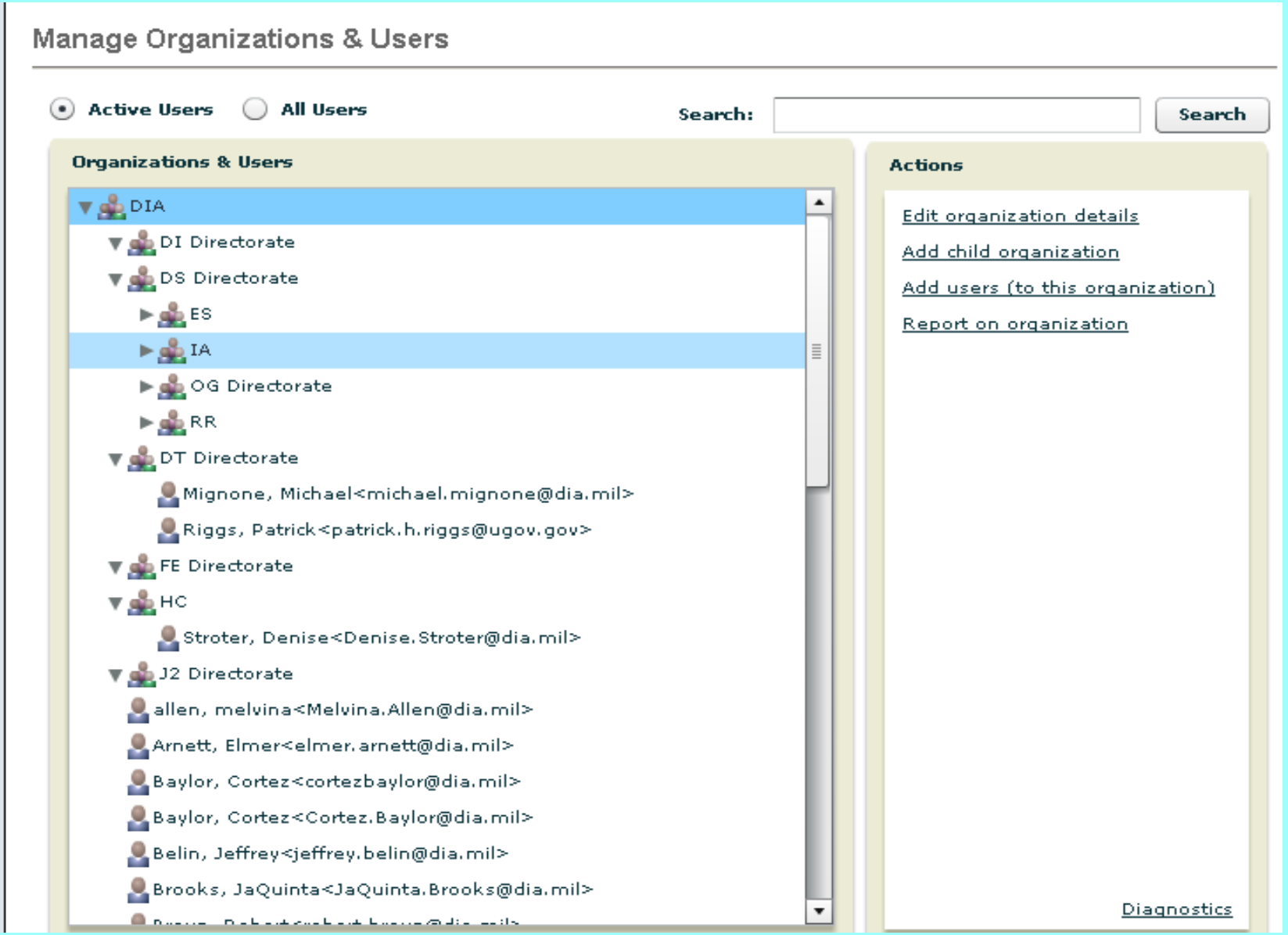
Public

Access FREE computer security and forensics training in the VTE Library.

- 200+ hours of lectures and demos from CERT
- No registration required!

Access the VTE Library

Software Engineering Institute | Carnegie Mellon


Manage Organizations & Users
Active Users
All Users
Search:
Search
Organizations & Users
DIA
DI Directorate
DS Directorate
ES
IA
OG Directorate
RR
DT Directorate
Mignone, Michael<michael.mignone@dia.mil>
Riggs, Patrick<patrick.h.riggs@ugov.gov>
FE Directorate
HC
Stroter, Denise<Denise.Stroter@dia.mil>
J2 Directorate
allen, melvina<Melvina.Allen@dia.mil>
Arnett, Elmer<elmer.arnett@dia.mil>
Baylor, Cortez<cortezbaylor@dia.mil>
Baylor, Cortez<Cortez.Baylor@dia.mil>
Belin, Jeffrey<jeffrey.belin@dia.mil>
Brooks, JaQuinta<JaQuinta.Brooks@dia.mil>
Actions
Edit organization details
Add child organization
Add users (to this organization)
Report on organization
Diagnostics

Security+ Prep

Description: This course prepares students to take the CompTIA Security DoD focus.

Progress: (0%)

Instructor: VTE Support (email) (Bio)

Office Hours: By request (email instructor)

Support Forum:

- Security+ Prep
  - Security+ Domain 1: General Security Concepts
    - Access Control Models [NC]
    - Methods of Authentication - Kerberos [NC]
    - Methods of Authentication – CHAP, Tokens, Multi-factor, Biometrics [NC]
    - Non-essential services [NC]
    - DEMO: Improving Security with Windows 2000 Group Policy [NC]
    - DEMO: Windows Security Templates [NC]
    - LAB: Enforcing Windows 2000 Security [NC]
    - LAB: Windows 2000 Host System Hardening [NC]
    - Attacks – DoS-DDos, Back Door [NC]
    - Attacks – Spoofing, Man in the Middle [NC]
    - DEMO: Man-in-the-middle Mitigation [NC]
    - DEMO: Analyzing Spoofed IP Addresses [NC]
    - DEMO: Spoofing MAC Address for ARP [NC]
    - Attacks – Replay, Social Engineering, Password Guessing, Software Exploitation [NC]
    - DEMO: Buffer Overflow [NC]
    - Malicious Code [NC]
    - Social Engineering [NC]
    - Auditing, Logging, and Scanning [NC]
    - DEMO: Vulnerability Assessment with Nmap [NC]
    - QUIZ: Security+ Domain 1 [NC]
  - Security+ Domain 2: Communication Security
    - Access Technologies – VPN, RADIUS, TACACS, L2TP-PPTP [NC]
    - Access Technologies – IPSec, SSH, Vulnerabilities [NC]
    - LAB: Multiplatform Traffic Encryption with IPSec [NC]
    - Email Security Concepts [NC]
    - DEMO: PGP Encryption [NC]
    - LAB: Encrypting Email and Files with GnuPG, Enigmail & Windows Privacy Tray [NC]

- LAB: Multiplatform Traffic Encryption with IPSec [NC]
- Email Security Concepts [NC]
- DEMO: PGP Encryption [NC]
- LAB: Encrypting Email and Files with GnuPG, Enigmail & Windows Privacy Tray [NC]
- LAB: Install and Configure a Spam and Virus Filtering Mail Relay [NC]
- Internet Security Concepts – SSL-TLS, HTTP-S [NC]
- Internet Security Concepts – Instant Messaging, Vulnerabilities [NC]
- Directory Security Concepts [NC]
- File Transfer Protocols [NC]
- Wireless Technologies [NC]
- QUIZ: Security+ Domain 2 [NC]

Security+ Domain 3: Infrastructure Security

- Infrastructure Security - Devices – Modems, RAS, Hubs, Switches, VPN [NC]
- Infrastructure Security - Devices – Routers, Firewalls [NC]
- Infrastructure Security - Devices – Network Monitoring, Workstations, Mobile Devices [NC]
- DEMO: Netstat & traceroute [NC]
- Infrastructure Security - Media – Coaxial, UTP-STP, and Fiber Optic cable [NC]
- Infrastructure Security - Media – Backups and Storage [NC]
- DEMO: Viewing the Windows archive bit [NC]
- Infrastructure Security -Media – Removable Media [NC]
- Security Topologies [NC]
- DEMO: Connection Limiting [NC]
- Intrusion Detection [NC]
- DEMO: Analysis Console for Intrusion Databases (ACID) [NC]
- LAB: Install and Configure Snort with ACID on Linux [NC]
- DEMO: Tripwire [NC]
- LAB: File Integrity Monitoring on Windows and Linux [NC]
- Security Baselines – Network-OS Hardening, Updates, Web server, Email, FTP [NC]
- Application Hardening – DNS, NNTP, File-Print, DHCP [NC]
- QUIZ: Security+ Domain 3 [NC]

- QUIZ: Security+ Domain 3 [NC]
- Security+ Domain 4: Cryptography
  - Introduction to Cryptography – Crypto Background [NC]
  - Introduction to Cryptography – Keys [NC]
  - Cryptographic algorithms -Hashing [NC]
  - DEMO: File Hashing [NC]
  - Cryptographic algorithms – Symmetric and Asymmetric [NC]
  - DEMO: Website asymmetric keys [NC]
  - Cryptography security concepts [NC]
  - Public Key Infrastructure (PKI) – Certification Authority, Policies, Key Distribution [NC]
  - Public Key Infrastructure (PKI) – Implementation, Trust Model [NC]
  - DEMO: Certificate Authority Issuance Number [NC]
  - LAB: Building a Microsoft PKI [NC]
  - Cryptographic standards and protocols [NC]
  - Key Management & Certificate Lifecycle [NC]
  - QUIZ: Security+ Domain 4 [NC]
- Security+ Domain 5
  - Physical Security – Physical barriers, access control [NC]
  - Physical Security- Social Engineering [NC]
  - Policies and Procedures [NC]
  - Privilege Management [NC]
  - Forensics [NC]
  - Risk Identification [NC]
  - Training and Awareness [NC]
  - Documentation Concepts [NC]
  - QUIZ: Security+ Domain 5 [NC]
- Security+ Review
  - Domain 1.0 Review - General Security Concepts [NC]
  - Domain 2.0 Review - Communication Security [NC]
  - Domain 3.0 Review - Infrastructure Security [NC]
  - Domain 4.0 Review - Basics of Cryptography [NC]
  - Domain 5.0 Review - Operational - Organizational Security [NC]
- Security+ Exam Quick Review Sheet [NC]
- QUIZ: Security+ Final [NC]

(ISC)2 TM CISSP (R) Prep

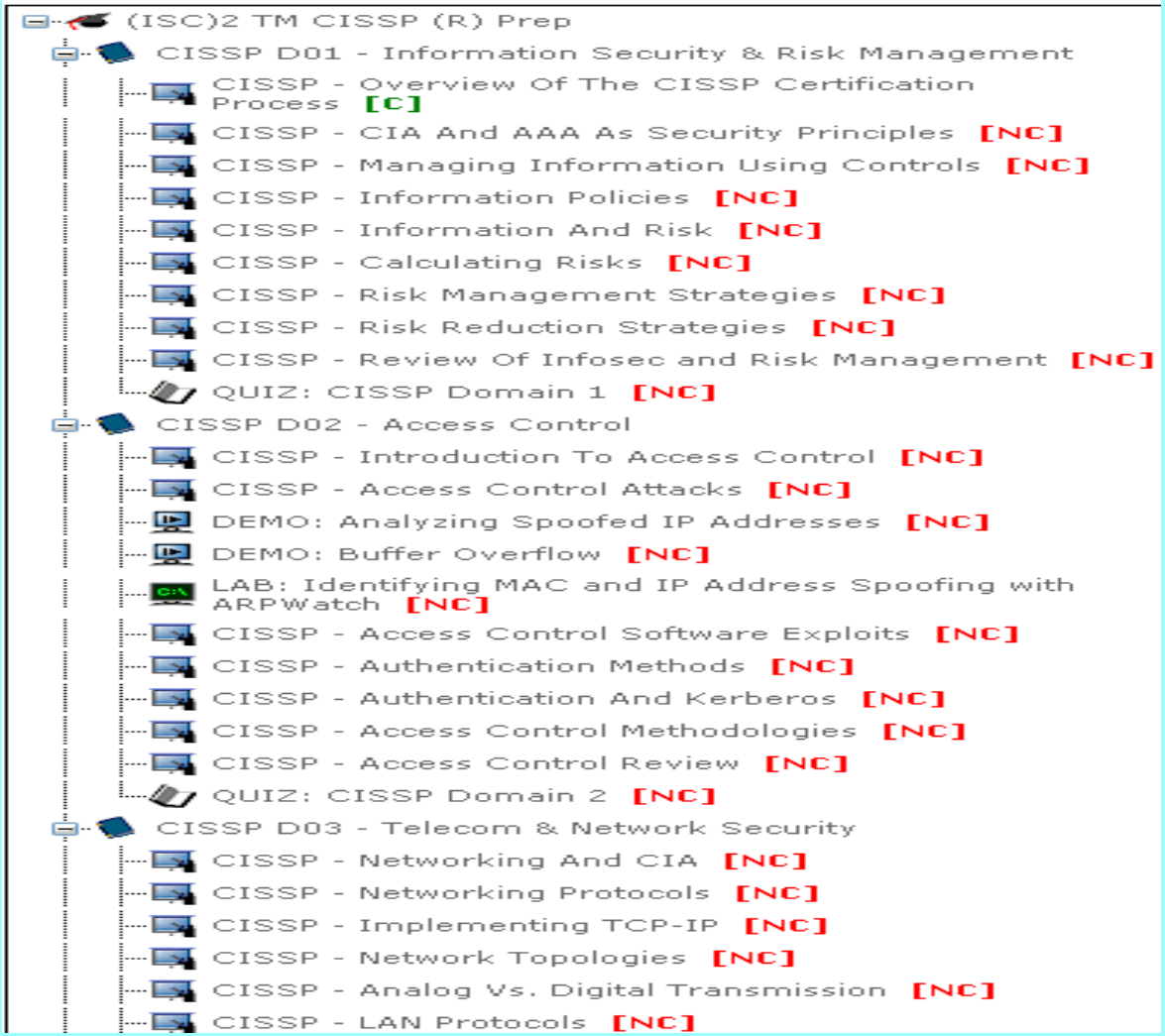
Description: This course is designed to support students working to acc

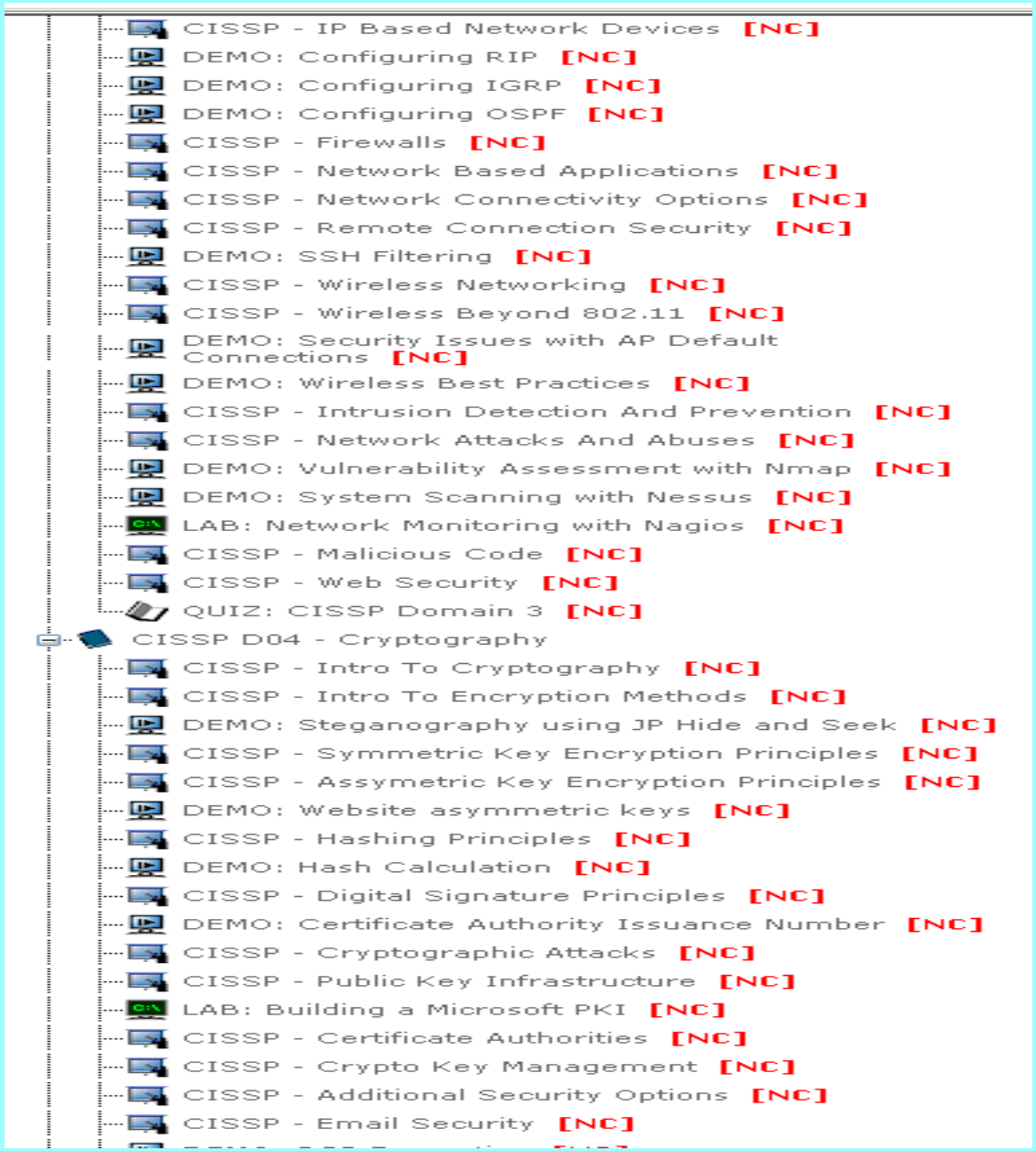
Progress: (1%)

Instructor: VTE Support (email) (Bio)

Office Hours: By request (email instructor)

Support Forum:




CISSP - IP Based Network Devices [NC]
DEMO: Configuring RIP [NC]
DEMO: Configuring IGRP [NC]
DEMO: Configuring OSPF [NC]
CISSP - Firewalls [NC]
CISSP - Network Based Applications [NC]
CISSP - Network Connectivity Options [NC]
CISSP - Remote Connection Security [NC]
DEMO: SSH Filtering [NC]
CISSP - Wireless Networking [NC]
CISSP - Wireless Beyond 802.11 [NC]
DEMO: Security Issues with AP Default Connections [NC]
DEMO: Wireless Best Practices [NC]
CISSP - Intrusion Detection And Prevention [NC]
CISSP - Network Attacks And Abuses [NC]
DEMO: Vulnerability Assessment with Nmap [NC]
DEMO: System Scanning with Nessus [NC]
LAB: Network Monitoring with Nagios [NC]
CISSP - Malicious Code [NC]
CISSP - Web Security [NC]
QUIZ: CISSP Domain 3 [NC]
CISSP D04 - Cryptography
CISSP - Intro To Cryptography [NC]
CISSP - Intro To Encryption Methods [NC]
DEMO: Steganography using JP Hide and Seek [NC]
CISSP - Symmetric Key Encryption Principles [NC]
CISSP - Assymetric Key Encryption Principles [NC]
DEMO: Website asymmetric keys [NC]
CISSP - Hashing Principles [NC]
DEMO: Hash Calculation [NC]
CISSP - Digital Signature Principles [NC]
DEMO: Certificate Authority Issuance Number [NC]
CISSP - Cryptographic Attacks [NC]
CISSP - Public Key Infrastructure [NC]
LAB: Building a Microsoft PKI [NC]
CISSP - Certificate Authorities [NC]
CISSP - Crypto Key Management [NC]
CISSP - Additional Security Options [NC]
CISSP - Email Security [NC]

- DEMO: PGP Encryption [NC]
- LAB: Encrypting Email and Files with GnuPG, Enigmail & Windows Privacy Tray [NC]
- CISSP - Wireless Security [NC]
- QUIZ: CISSP Domain 4 [NC]
- CISSP D05 - Security Architecture and Design
  - CISSP - Systems Architecture [NC]
  - CISSP - Architecture Protection [NC]
  - QUIZ: CISSP Domain 5 [NC]
- CISSP D06 - Operations Security
  - CISSP - Introduction To Operations Security [NC]
  - CISSP - Life Cycle Processes And Controls [NC]
  - CISSP - Monitoring And Auditing [NC]
  - CISSP - Threats, Vulnerabilities And Countermeasures [NC]
  - QUIZ: CISSP Domain 6 [NC]
  - LAB: Vulnerability Assessment with Nessus [NC]
- CISSP D07 - Applications Security
  - CISSP - The Life Cycle Model [NC]
  - CISSP - Coding And Data Storage Systems [NC]
  - QUIZ: CISSP Domain 7 [NC]
- CISSP D08 - BCP and Disaster Recovery Planning
  - CISSP - Business Continuity and Disaster Recovery [NC]
  - CISSP - The Four Elements Of Business Continuity [NC]
  - CISSP - Disaster Recovery Planning [NC]
  - CISSP - The Data Processing Continuity Plan [NC]
  - CISSP - DRP Maintenance And Testing [NC]
  - CISSP - Data Recovery Roles And Procedures [NC]
  - QUIZ: CISSP Domain 8 [NC]
- CISSP D09 - Law, Investigation, and Ethics
  - CISSP - Introduction To Computer Crime [NC]
  - CISSP - Computer Crime Issues [NC]
  - CISSP - Cyber Investigations [NC]
  - QUIZ: CISSP Domain 9 [NC]
- CISSP D10 - Physical Security
  - CISSP - Physical Security Plans [NC]
  - CISSP - Environmental And Life Safety Controls [NC]
  - CISSP - Physical And Technical Controls [NC]
  - QUIZ: CISSP Domain 10 [NC]
- CISSP Final
  - CISSP Review Guide [NC]
  - QUIZ: CISSP Final [NC]

XYZ Corp
222 contractor way,
Contractorville, MD
Attention: _____
Dear _____

Subject: Request for Information Regarding Information Assurance Workforce Certifications

As you may be aware, DoD 8570.1-M is a recent initiative to strengthen information assurance programs throughout the Department of Defense. DoD 8570.1-M categorizes information assurance workforce functions and establishes certification standards for each information assurance workforce functional category. DIA is implementing DoD 8570.1-M in a phased approach, and while it is not yet formally invoked across our contractor base, to assist us with our readiness reporting, we are seeking information, on a voluntary, no-cost basis, from current contractors who are performing information assurance tasks for DIA. Your company has been identified as a DIA contractor performing information assurance tasks that fall within the functional categories described in DoD 8570.1-M. As such, your participation in this survey will enhance DIA's information assurance posture reportable under DoD 8570.1-M and FISMA requirements.

Attached to this letter is a spreadsheet identifying the members of your current workforce, including any known subcontractors, performing tasks under contract number HHM402-xx-x-xxxx. We have assessed the tasks performed on the contract against the information assurance workforce functional categories described in DoD 8570.1-M, and have indicated the pertinent certifications that DoD 8570.1-M requires for the functional category we have associated with that individual's contractual effort. Please identify which, if any, of the pertinent certifications are currently held by these individuals; the dates the certifications were obtained; and, if available, the 5-digit reference number assigned by the certification provider.

We would very much appreciate your participating in this survey; however, please note that your decision to participate is strictly voluntary. The Government will not compensate you for your participation. Accordingly, by responding, you agree that any action taken pursuant to this request will not result in a change to any Government contract or in costs being charged to any Government contract, and that the Government may freely use any of the information you provide, without restriction, to address information assurance readiness and reporting requirements of the DoD and DIA. If you do not agree to the foregoing, please notify the DIA contracting officer and take no action in response to this request. If you choose to participate, please provide the information by annotating the worksheet and emailing it to Mr. Paul Krasley at paul.krasley@dia.mil by January 11, 2008.
If you have any questions regarding this request, call contact Joe Contracting Officer, 202-…… or Paul Krasley, 202-231-2387.

Attachment: Example of Contractor Data: One for each Vendor

Register Now! for SANS Training

SANS OnDemand Assessments - Webcast Classroom Training

Please Note: You have 10 minutes to complete this page. After 10 minutes have passed you will have to restart this page.

Registration Form

You are logged in.

Click HERE to log out, or to register someone other than yourself.

Step 1: Attendee's Mailing Address

READ THIS IMPORTANT NOTICE

This section is for the student's contact info. The e-mail address provided in this step is where all access information will go.

The student's address must be entered here correctly as it can not be changed once access to courseware has been granted.

Common Errors To Avoid:

- Entering your work email, but wanting access to be with a personal address or vice versa.
- Entering your email when you are registering someone else
- Entering your address to get a confirmation email even though you are registering another person. If you need a copy of the confirmation emails, enter your e-mail in the billing contact field on the next page of the process.

Separate billing information may be entered later in the registration process if needed.

* Attendee's E-Mail:	paul.krasley@dia.mil
* Attendee's E-Mail (repeat):	paul.krasley@dia.mil
Salutation:	
* First Name:	Paul
* Last Name:	Krasley
* Title:	IA Training
* Company:	DIA
* Address:	5403 Castle Bar Lane
Address (cont.):	
* City:	Alexandria
* ZIP/Postal Code:	22315
* State:	Virginia
* Country:	United States
* Phone:	2022312387

https://www2.sans.org/ondemand/choose.php

Course	
☐ AUD 507: Auditing Networks, Perimeters & Systems ($179)	
☐ SEC 309: Intro to Information Security ($179)	GISF
☐ SEC 333: SANS Training for the CompTIA Security+ Certification ($179)	
☐ SEC 351: Computer and Network Security Awareness ($29)	
☐ SEC 401: SANS Security Essentials ($179)	GSEC
☐ SEC 430: Windows SysAdmin Essentials ($59)	
☐ MGT 411: SANS 17799/27001 Security & Audit Framework ($179)	CISSP
☐ MGT 414: SANS® +S™ Training Program for the CISSP® Certification Exam ($179)	
☐ MGT 421: SANS Leadership and Management Competencies ($59)	
☐ SEC 502: Perimeter Protection In-Depth ($179)	
☐ SEC 503: Intrusion Detection In-Depth ($179)	GCIA for CND
☐ SEC 504: Hacker Techniques, Exploits & Incident Handling ($179)	GCIH for CND
☐ SEC 505: Securing Windows ($179)	
☐ SEC 508: System Forensics, Investigation & Response ($179)	
☐ MGT 512: SANS Security Leadership Essentials For Managers with Knowledge Compression™ ($179)	GSLC
☐ MGT 524: Security Policy & Awareness ($179)	
☐ SEC 617: Assessing and Securing Wireless Networks ($179)	
Total Course Fee	Review (click to update total)

Proceed Review

Step 3: Discount Codes

Registration code (for discount): DoD8570

Note: You must submit your discount code at the time of your original registration. SANS can not modify your tuition fee once you have submitted this form. See www.sans.org/conference/discount.php for more information or to obtain a code.

Proceed Review

ALL FEES ARE QUOTED IN US DOLLARS & MUST BE PAID IN US DOLLARS

Total Fee: $0.00

Enter your name if you would like it to appear on your assessment results: :

1. Which of the following would BEST ensure the success of information security governance within an organization?

- A. The steering committee approves all security projects.
- B. The security policy manual is distributed to all managers.
- C. Security procedures are accessible on the company intranet.
- D. The corporate network utilizes multiple screened subnets.

2. Which of the following should be developed FIRST?

- A. Standards
- B. Procedures
- C. Policies
- D. Guidelines

3. Which of the following individuals would be in the BEST position to sponsor the creation of an information security steering group?

- A. Chief security officer
- B. Chief operating officer
- C. Chief internal auditor
- D. Chief legal counsel

4. Which of the following would normally be covered in an insurance policy for computer equipment coverage? Equipment:

- A. leased to the insured by another company.
- B. leased to another company by the insured.
- C. under the direct control of another company.
- D. located at and belonging to a service provider.

5. The MOST appropriate reporting base for the information security management function would be to report to the:

- A. head of IT.
- B. infrastructure director.
- C. network manager.
- D. chief information officer.

50. Which of the following should be mandatory for any disaster recovery test?

- A. Only materials taken from offsite storage or those predeployed at the hot site are used.
- B. Participants are not informed in advance when the test is to be held.
- C. Hot site personnel are not informed in advance when the test is to be held.
- D. Key systems are restored to identical operating system (OS) releases and hardware configurations.

Check My Score | Reset **Results will appear in a new window.**

1. Enter your name
2. Answer each question
3. Check your Answers

http://www.isaca.org/Template.cfm?Section=CISM_Certification&CONTENTID=28399&TEMPLATE=/ContentManagement/ContentDisplay.cfm.

COMPTIA

- http://currency.comptia.org/dod

- Tara Dean: tdean@comptia.org (732) 662-4020

- Agency User name: dia
- Password: xxxxxxxx

- PC Technician = A+
- Network Technologies = Network +
- IT Security = Security +

DEPARTMENT OF DEFENSE PERSONNEL CERTIFICATION SUPPORT SYSTEM

Home FAQs Contact Us E-Support

INFORMATION ASSURANCE (IA)

- About IA
- IA Policy/Resources
- PCSS IAM Login
- IA Reporting Login
- OPR POC Login
- Downloads

CERTIFICATION PROGRAMS

- IA WIP Certification Request
- DANTES Microsoft Pilot

Returning User Login

** Your session has timed out, please login again. **

Email address:

Password: Forgot your Password?

LOGIN

New User Registration

Don't have an account on the Personnel Certification Support System?

You can get registered now! It only takes about five (5) minutes to complete your registration.

BEGIN REGISTRATION PROCESS

IAM Registration

If you would like to be listed as an IAM for your component, you can self-register here. Your account will be activated once it is approved by your component's OPR POC.

BEGIN REGISTRATION PROCESS

DEPARTMENT OF DEFENSE PERSONNEL CERTIFICATION SUPPORT SYSTEM

Home | FAQs | Contact Us | E-Support

INFORMATION ASSURANCE (IA)

- About IA
- IA Policy/Resources
- PCSS IAM Login
- IA Reporting Login
- OPR POC Login
- Downloads
- Log Off

CERTIFICATION PROGRAMS

- IA WIP Certification Request
- DANTES Microsoft Pilot

Paul Krasley's Management Page

[Reporting | Edit My Profile | Log Off]

Vouchers Awaiting Approval

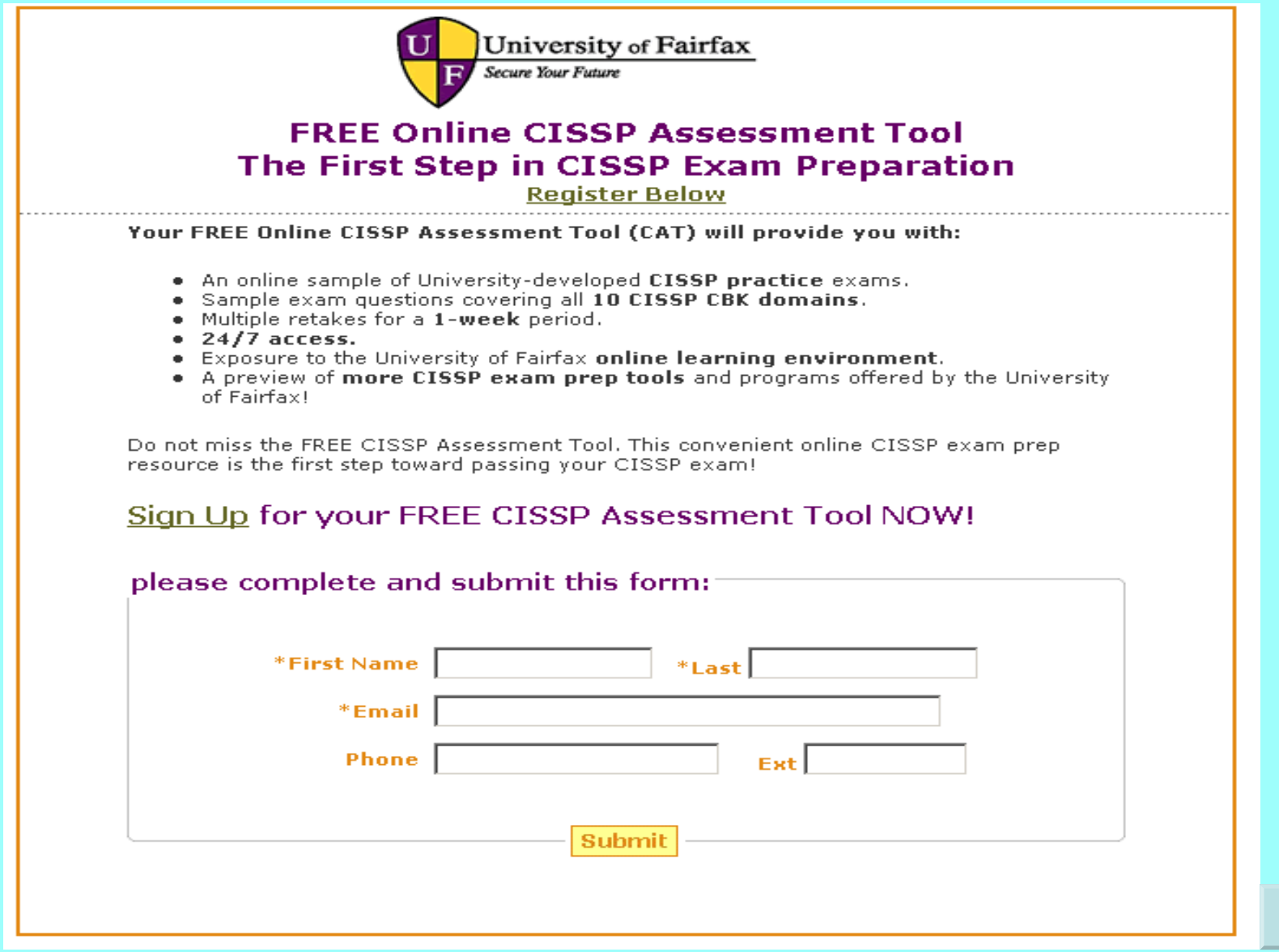
Name	Command & Unit/Org	Contact	IA Level	Exam
No Vouchers Pending Approval				

My IAM Group

With the checked Users: - Actions -

	Name	Command & Unit/Org	Contact	IA Level	Exams
☐	Adams, William P		Send Email 202-231-2021	IAM III	Certified Information Systems Security Professional Exam
☐	Cornell, Denise		Send Email 202.231.3524	IAM III	
☐	Kelchner, Willard F		Send Email 301 306 6128	IAM III	Certified Information Systems Security Professional Exam
☐	martin, jerome		Send Email (202)231-8816	IAT III	Certified Information Systems Security Professional Exam
☐	Quinn, Robert		Send Email 202-231-3890	IAM III	GIAC Security Leadership
☐	Scott, Jonathan C		Send Email 7195548549	IAM III	Certified Information Systems Security Professional Exam
☐	Stroter, Denise Y		Send Email 2022312981	IAT III	Certified Information Systems Security Professional Exam
☐	Westray, Jr., Derek H	DS/RR RRC-2	Send Email 301-306-6166	IAT III	Certified Information Systems Security Professional Exam

http://www.ufairfax.net/ufairfax/lp/examprep.html



Thank You

Dear Paul:

Congratulations! By registering for the **Free CISSP Assessment Tool** (CAT) offered by the ***University of Fairfax***, you have taken the first step toward passing your CISSP exam.

You will have access to the Free CAT for a period of one week. Your enrollment period will begin on the Friday following your registration.* For example, if today is Friday, you will be enrolled in one week. However, if today is Thursday, you will be enrolled tomorrow.

On your first day of enrollment, login instructions will be emailed to username@domain.suffix. As soon as you receive an email with login instructions, you may immediately log into the FREE CISSP Assessment Tool.

* If a holiday occurs on a Friday, you will receive online access prior to the holiday. Please see below a list of holidays observed by the University of Fairfax.

- Martin Luther King Jr. Day
- Memorial Day
- Independence Day
- Labor Day
- Thanksgiving Day & the day after
- Christmas Day
- New Year's Day

Best regards,

Juliette Goldman
Associate Dean of Continuing Professional Education
University of Fairfax

Ready for an in-depth online CISSP exam prep program? Click here!

Click here to review all of our CISSP test prep options.

BECOME AN INFOSEC LEADER!

The University of Fairfax provides the following programs to help you advance your InfoSec career.

- **NSA IAM-IEM Certification Courses**:

  To support the **NSA IAM/IEM** certification program, the University of Fairfax, in conjunction with Security Horizon, is awarding **scholarships** for **IAM/IEM Certification Courses**. The National Security Agency offers the only INFOSEC certification(s) sponsored by a federal agency. The NSA IAM and IEM certifications employ and teach a standardized INFOSEC assessment methodology. Click here for more information.