Building the Next Generation of Cyber Defenders

Tapping into the League of Wounded Warriors to help Protect and Defend the Nation's Information Systems

Sam Maroon
Jim Wiggins

Wounded Warrior
Cyber Combat Academy

FITSI
FEDERAL IT SECURITY INSTITUTE
HELPING SECURE THE NATION'S FEDERAL INFORMATION SYSTEMS

FITSI
- FOUNDATION -

Speaker Introduction

- Mr. Sam Maroon
  - Technical Instructor at the Foreign Service Institute (FSI) for the U.S. Department of State
  - Former Electronics Warfare Officer
  - Former Tactics Officer – Desert Storm
  - Graduate of Virginia Military Institute – BS Engineering
  - Graduate of George Washington University – Master's Certificate

- Mr. Jim Wiggins
  - Executive Director of the Federal IT Security Institute and the FITSI Foundation
  - Cybersecurity Trainer and Information Security Practitioner
  - 16 of experience in IT
  - 12 of experience in IT security
  - 2010 FISSEA "Educator of the Year Award"

Overview

- The Idea…
- Why?
- What?
- How?

The Idea…

- The Three Wise Men…
  - David
    - November 2009
  - Sam
    - Fall of 2011
  - Manny
    - February of 2012

Greek Wise Men

- All of them posed the same question:
  - Can’t we train Wounded Warriors in cybersecurity?

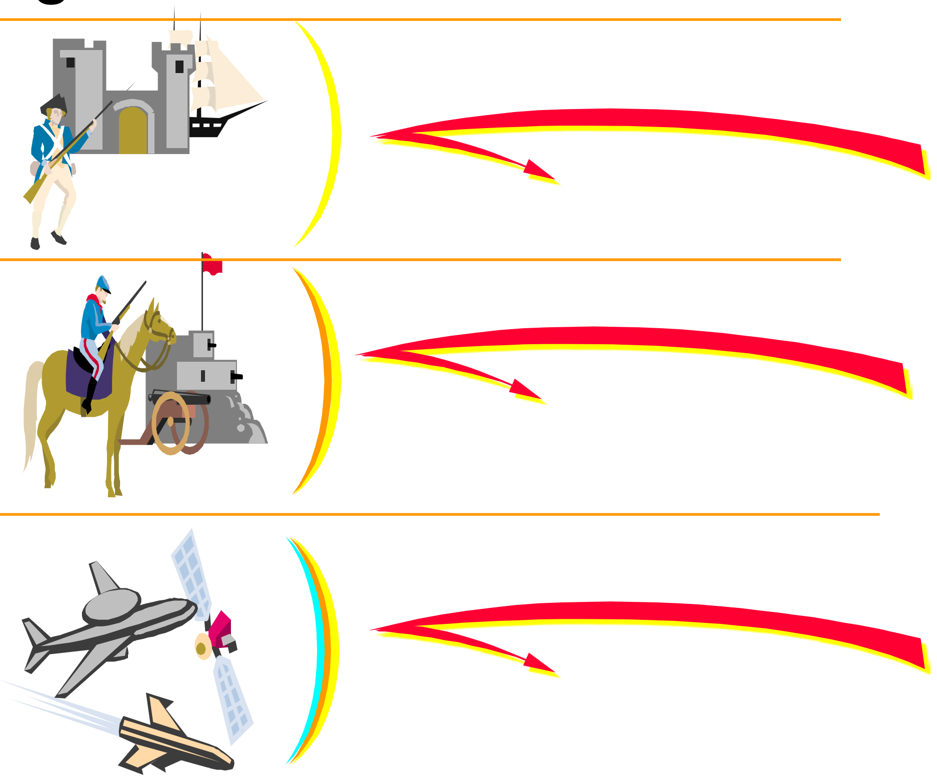
The Cybersecurity Problem Space

- Historic Background

18th Century

19th Century

20th Century

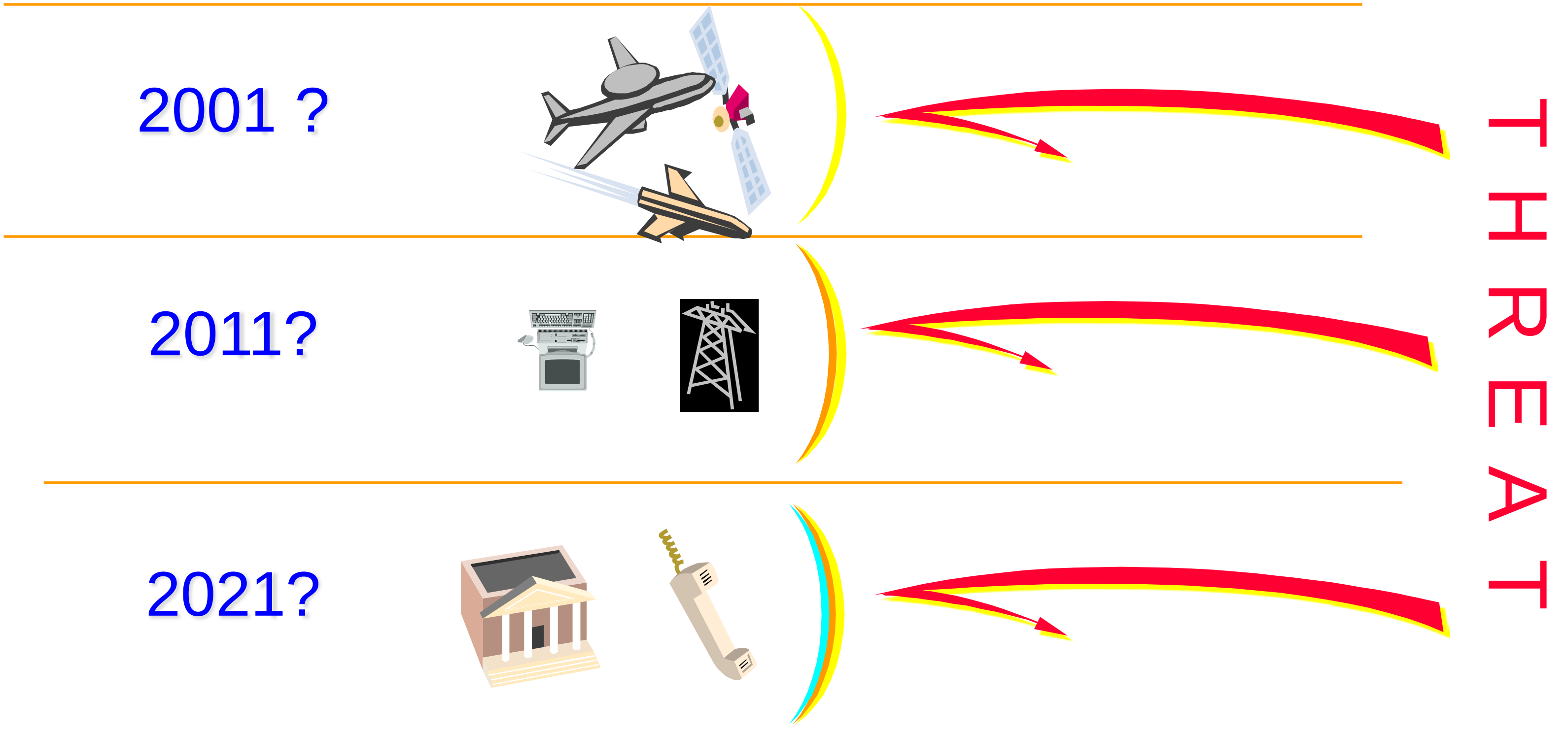


THREAT

Always a Target, But Always Defendable

The Cybersecurity Problem Space

- Where are we headed?



2001 ?

2011?

2021?

THREAT

Have We Lost The Advantage of Our Geography?

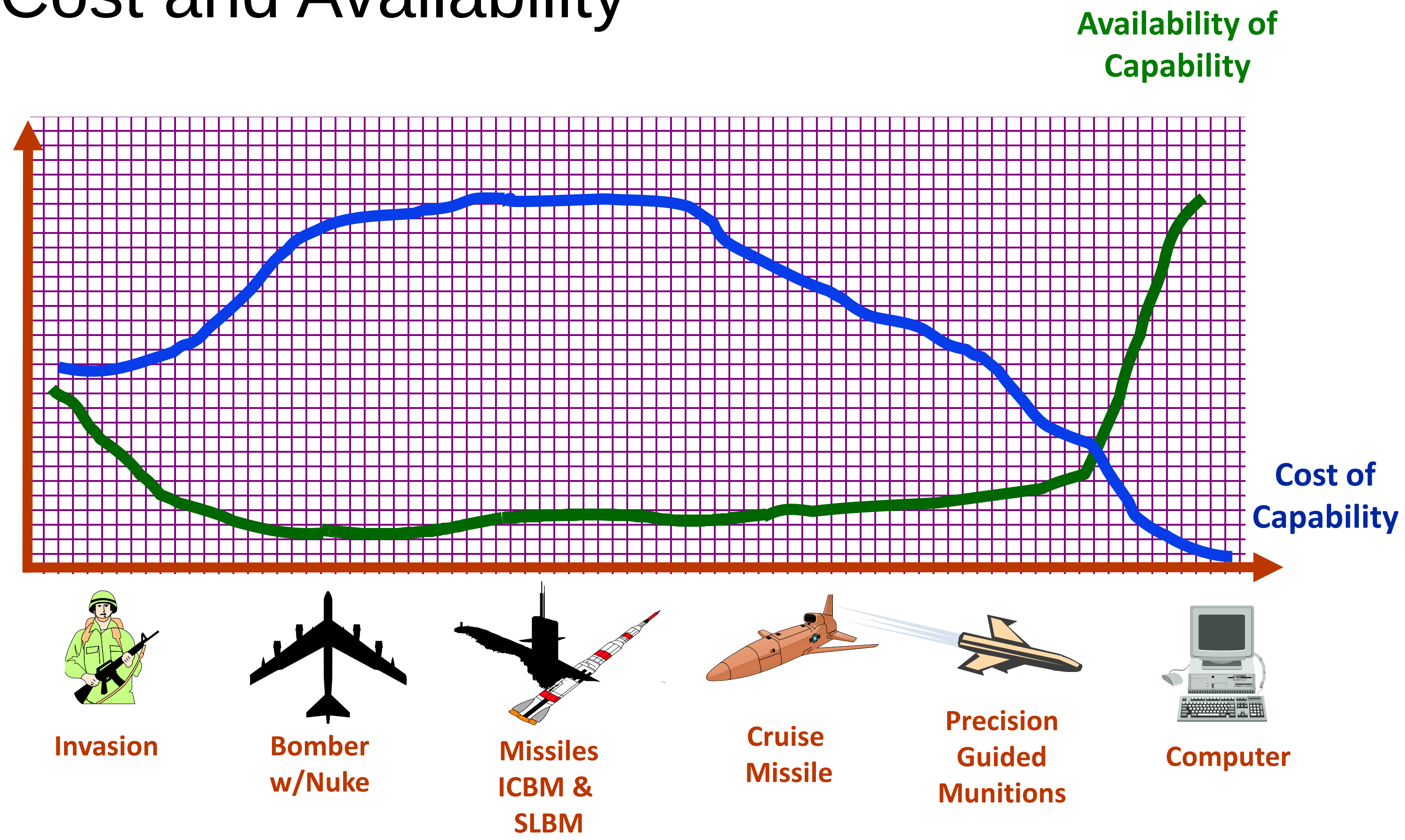
The Cybersecurity Problem Space

- Basis for Change

Information	▶	Property & Commodity
Network Connectivity	▶	New Benefits/New Risks
Globalization	▶	World-wide Competition
Cyber Dimension	▶	No Protecting Borders
Deregulation/Restructuring	▶	Potential Vulnerabilities
Military Superiority	▶	Asymmetric Warfare
Pace of Change	▶	Assimilation Problems

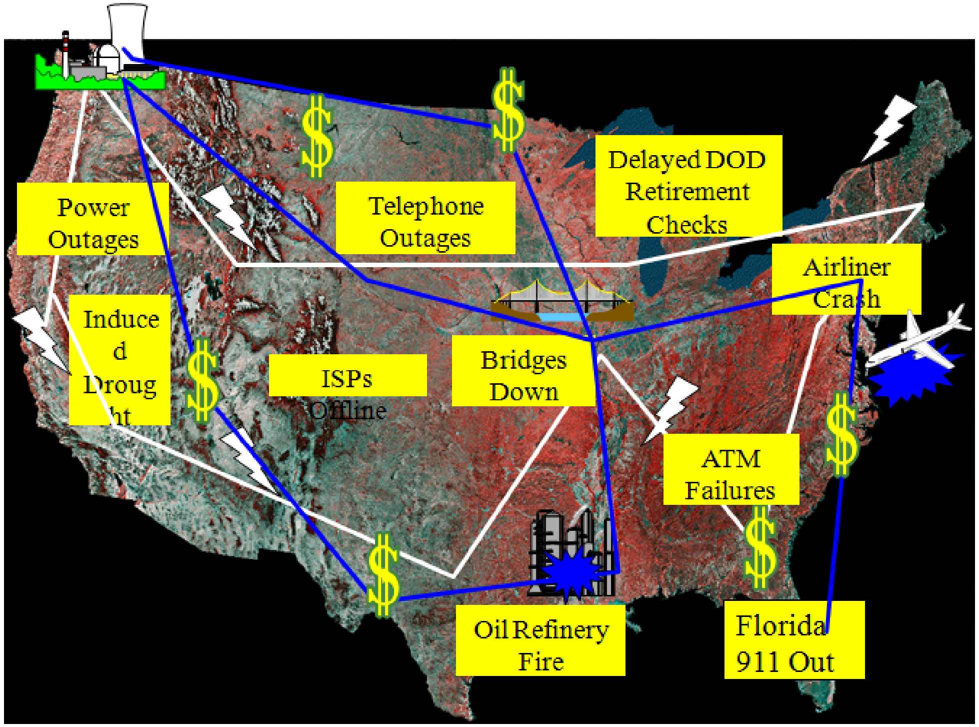
The Cybersecurity Problem Space

- Cost and Availability



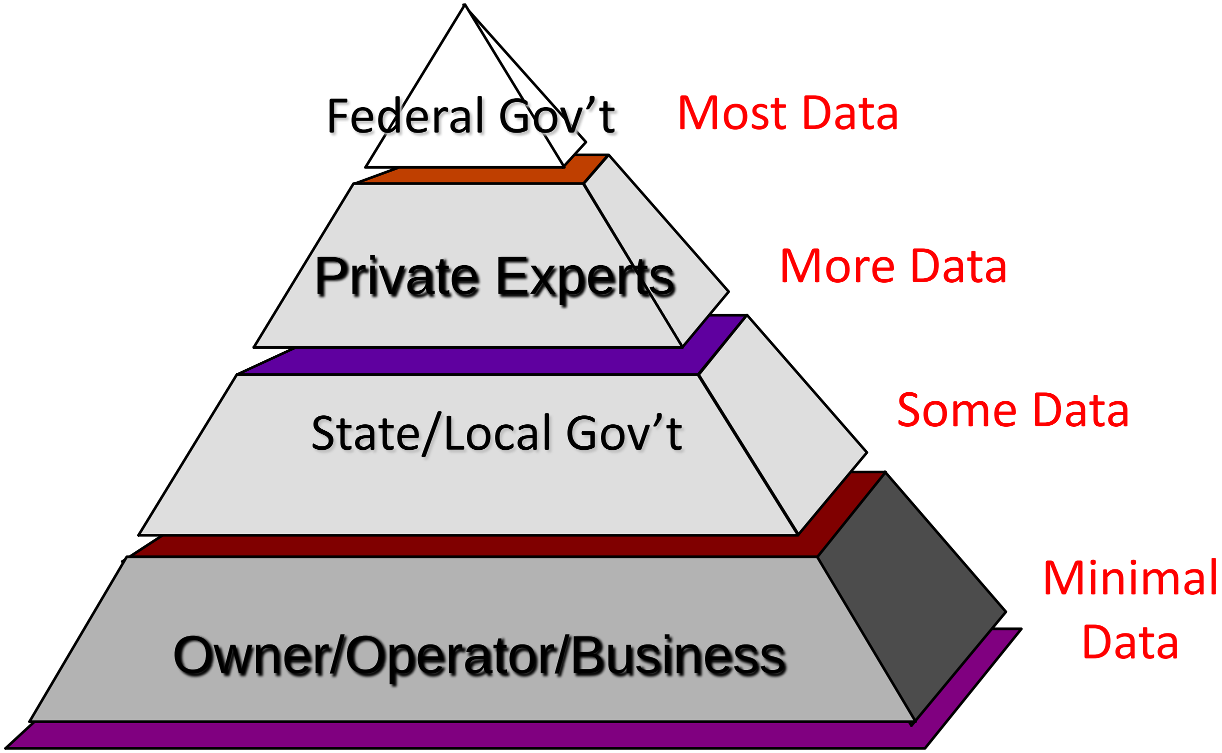
The Cybersecurity Problem Space

- Attack Recognition and Attribution



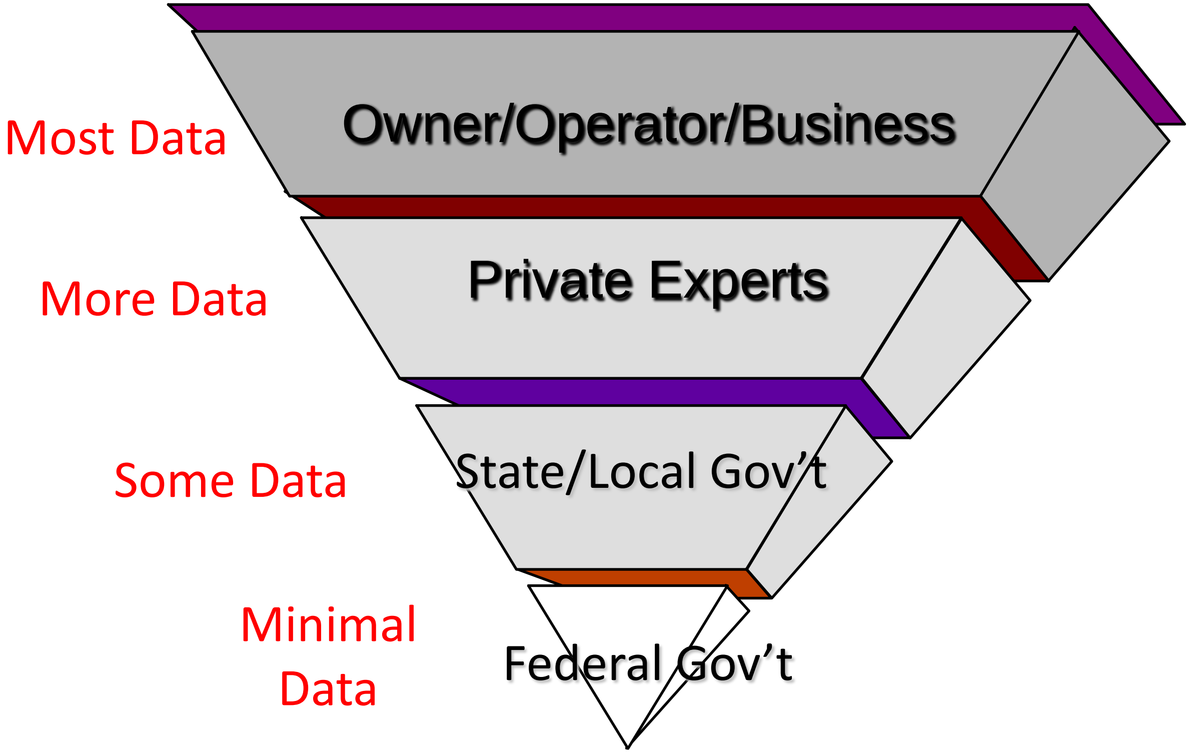
The Cybersecurity Problem Space

- Consider the Traditional National Security Model



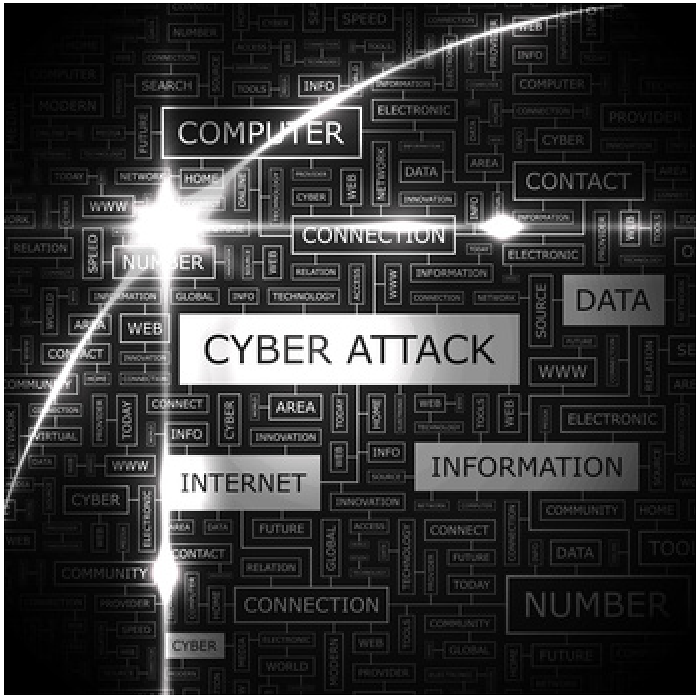
The Cybersecurity Problem Space

- Today's Cyber Security Model Stands the Traditional Model on Its Head!



The Need for Technical Cyber Defenders

- Cyber attacks continue to escalate
  - RSA
  - Oak Ridge National Laboratory
  - Many government contracting firms
- Attacks are highly sophisticated
  - Not just Denial of Service
  - Data theft and intellectual property being lost
    - i.e. - Advanced Persistent Threat



The Need for Technical Cyber Defenders

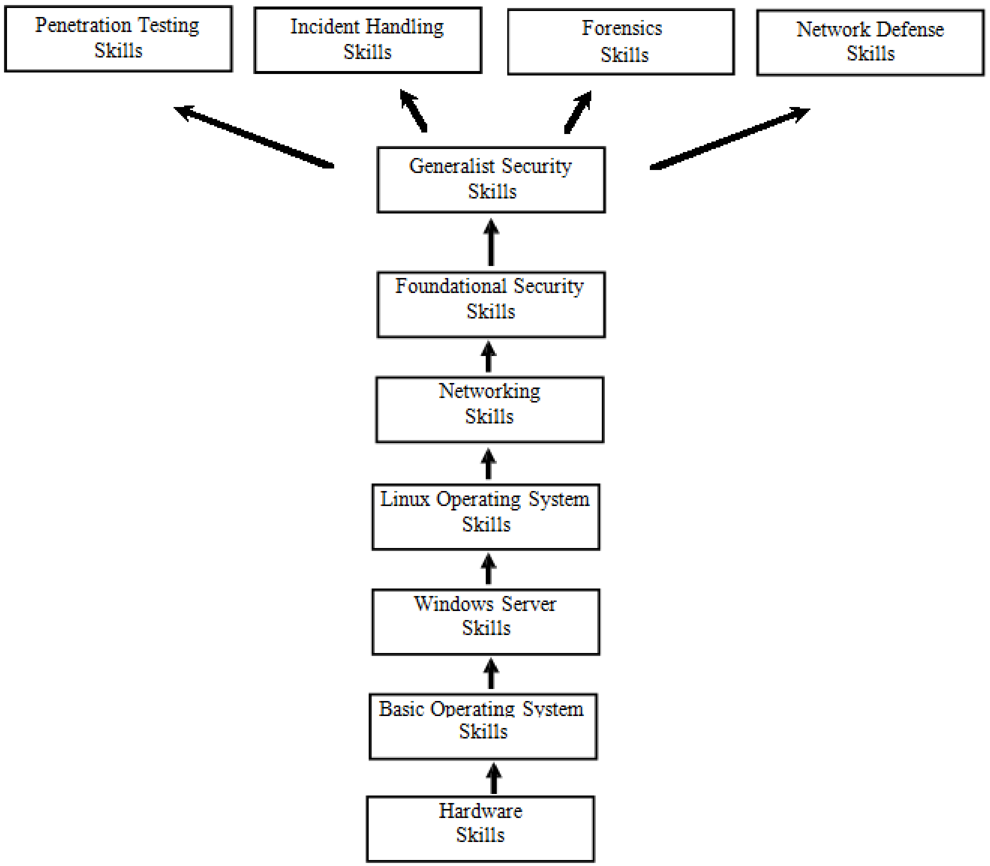
- In 2010, James Gosler, a veteran cyber security specialist who has worked at the CIA, the National Security Agency and the Energy Department made the following comment:
  - *"We don't have sufficiently bright people moving into this field to support those national security objectives as we move forward in time."*
    - Estimated that there were only 1,000 people in the entire United States with the necessary skills
    - A force of 20,000 to 30,000 skilled specialists is needed.[1]

[1] http://www.npr.org/templates/story/story.php?storyId=128574055

Building Technical Cyber Capabilities

- Lots of skills are required
  - Hardware Skills
  - Operating System Skills
  - Server Skills
  - Linux Skills
  - Networking Skills
  - Foundational Security Skills
  - Generalist Security Skills
  - Specialty Skills
    - Penetration Testing
    - Network Defense
    - Incident Handling
    - Forensic Analysis
    - Security Control Assessors

Building Technical Cyber Capabilities



Penetration Testing Skills
Incident Handling Skills
Forensics Skills
Network Defense Skills
Generalist Security Skills
Foundational Security Skills
Networking Skills
Linux Operating System Skills
Windows Server Skills
Basic Operating System Skills
Hardware Skills

The League of Wounded Warriors

- Who is a Wounded Warrior?
  - Military service members who have suffered a serious life altering injury
    - In combat or non-combat situations
    - Injury typically ends their ability to continue to serve
    - Mostly served in Iraq or Afghanistan

The League of Wounded Warriors

- What makes a wounded warrior an ideal candidate as a cyber defender?
  - Ability to be trained
  - Highly patriotic
  - Availability of time
  - Desire to repatriate
  - Aptitude for tactics and strategy
  - The Nation needs them

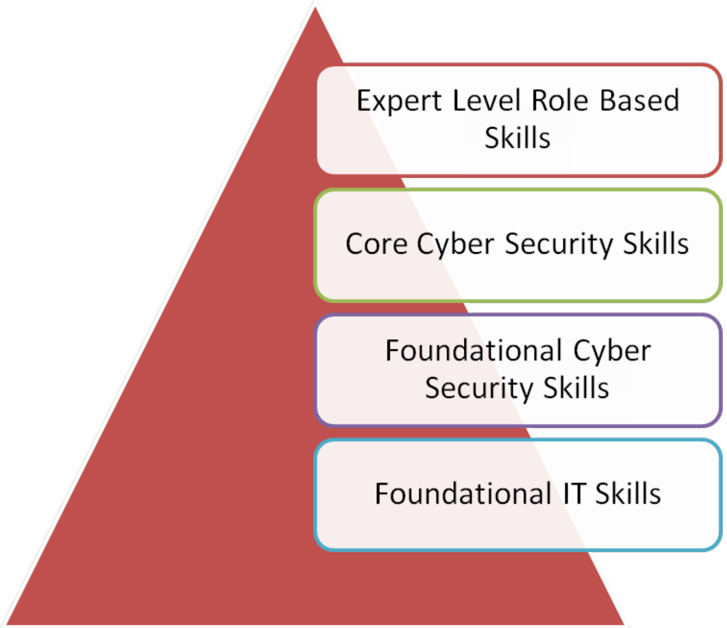
- They are dedicated, highly motivated, disciplined, and trustworthy team players who both industry and government seek as workers.

Wounded Warrior Training Model

- High Level Overview
- Use of Industry Certifications
- Use of Online Training Platform
- Use of a Cyber Range
- Use of Performance Based Assessments
- How the Pieces Fit Together

Wounded Warrior Training Model

- High Level Overview

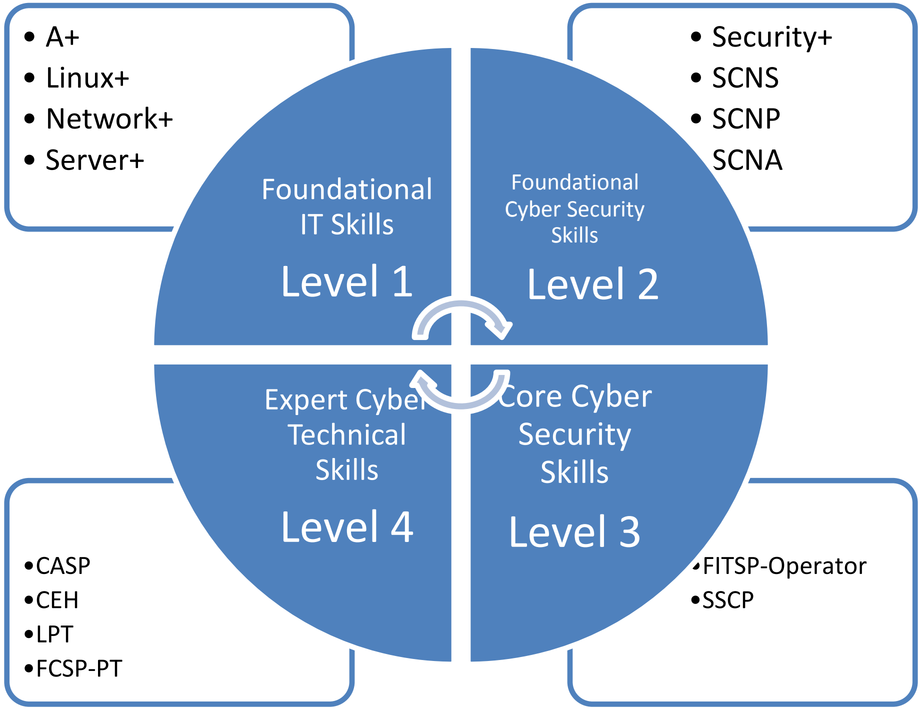

Expert Level Role Based Skills
Core Cyber Security Skills
Foundational Cyber Security Skills
Foundational IT Skills

Wounded Warrior Training Model

- Use of Industry Certifications
  - CompTIA
    - A+, Network+, Security+, Linux+, Server+, CASP
  - EC-Council
    - Certified Ethical Hacker, Licensed Penetration Tester
  - FITSI
    - FITSP-Operator
  - ISC2
    - Systems Security Certified Practitioner
  - Security Certified
    - Security Certified Network Specialist
    - Security Certified Network Professional
    - Security Certified Network Architect

Wounded Warrior Training Model

- Use of Industry Certifications



- A+
- Linux+
- Network+
- Server+

Foundational IT Skills

Level 1

- Security+
- SCNS
- SCNP
- SCNA

Foundational Cyber Security Skills

Level 2

Core Cyber Security Skills

Level 3

- FITSP-Operator
- SSCP

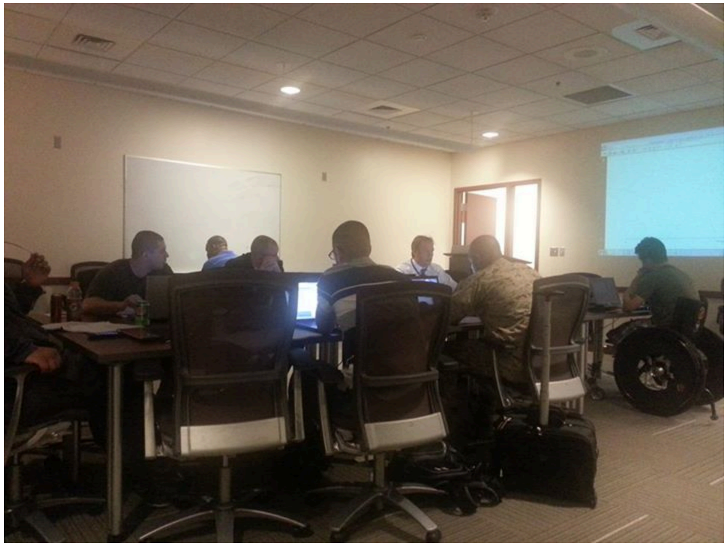
Expert Cyber Technical Skills

Level 4

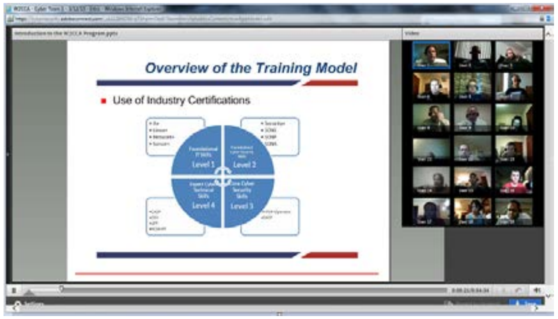
- CASP
- CEH
- LPT
- FCSP-PT

Wounded Warrior Training Model

- Hybrid Training Platform



Traditional Classroom

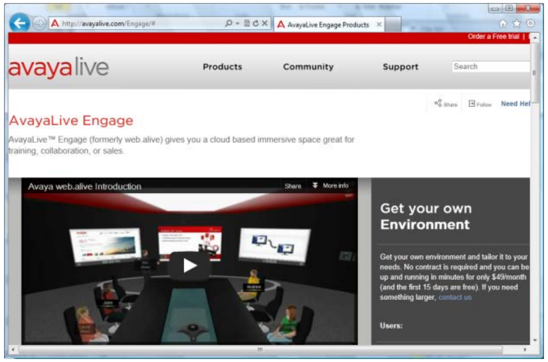


Introduction to the WCCCA Program.pptx

Video

Overview of the Training Model

- Use of Industry Certifications



http://avayalive.com/Engage/#

AvayaLive Engage Products

Order a Free trial |

avayalive

AvayaLive Engage

AvayaLive™ Engage (formerly web.alive) gives you a cloud based immersive space great for training, collaboration, or sales.

Avaya web.alive Introduction

Get your own Environment

Get your own environment and tailor it to your needs. No contract is required and you can be up and running in minutes for only $49/month (and the first 15 days are free). If you need something larger, contact us

Users:

Online Classroom

Wounded Warrior Training Model

- Use Cyber Range Technologies

Figure 1

AVAILABLE IA/CND TOOLS

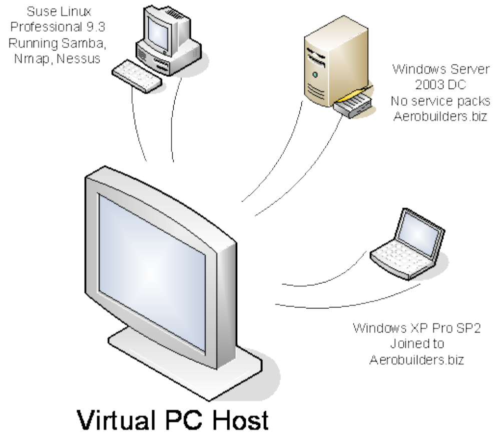
- ArcSight
- Sourcefire
- HBSS
- Splunk
- Wireshark
- Palo Alto
- Securify
- DoD Assured Compliance Assessment Solution (ACAS)
- IPSonar
- NIKSUN

ENVIRONMENT FEATURES

- Multi-protocol Label Switching (MPLS) Cloud
- Defense Enterprise Computing Centers (DECC) and Community Data Center (CDC), Internet Access Point, Multi-WAN Transport
- Base boundary defense
- Base network infrastructure
- Virtual actors
- Full Microsoft Office suite
- Numerous operating systems

ENVIRONMENT FEATURES

- Virtual Internet
  - Hundreds of sites
  - Full Domain Name System (DNS) replication
- Network- and host-based traffic generation
- Malicious content
- Boundary defense
- Real Hardware
- Various Security Technical Implementation Guides (STIG) configurations


Suse Linux Professional 9.3 Running Samba, Nmap, Nessus
Windows Server 2003 DC No service packs Aerobuilders.biz
Windows XP Pro SP2 Joined to Aerobuilders.biz
Virtual PC Host

Wounded Warrior Training Model

- Curriculum and Exercises on the Cyber Range

Role on the Cyber Range	**Certification program**
Help desk technician	A+
Network administrator	Network+
Network engineer	Server+
Network engineer	Linux+
Security Analyst	Security+
Security Administrator	SCNS
Security Engineer	SCNP/SCNA
Information Assurance Manager	CISSP
Information Systems Security Officer	FITSP-Operator
Blue Team Member	CEH
Red Team Member	ECSA/FCSP-Penetration Tester

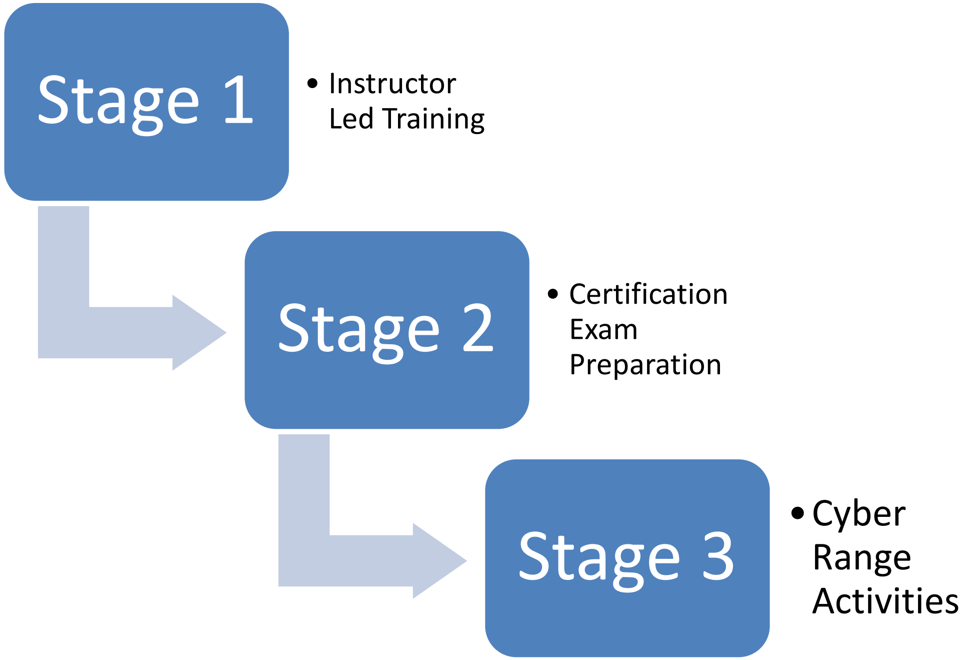
Wounded Warrior Training Model

- Use of Performance Based Assessments
  - Capstone for all graduates of the program
  - Exercises as part of the cyber range will train towards preparation of the capstone project
  - Can help demonstrate that the students can actually “do the work”
  - Will earn a final certification
    - Federal Cyber Security Professional - Penetration Tester

FCSP
Federal Cyber Security Professional
Penetration Tester

Wounded Warrior Training Model

- How the Pieces Fit Together



Program Details

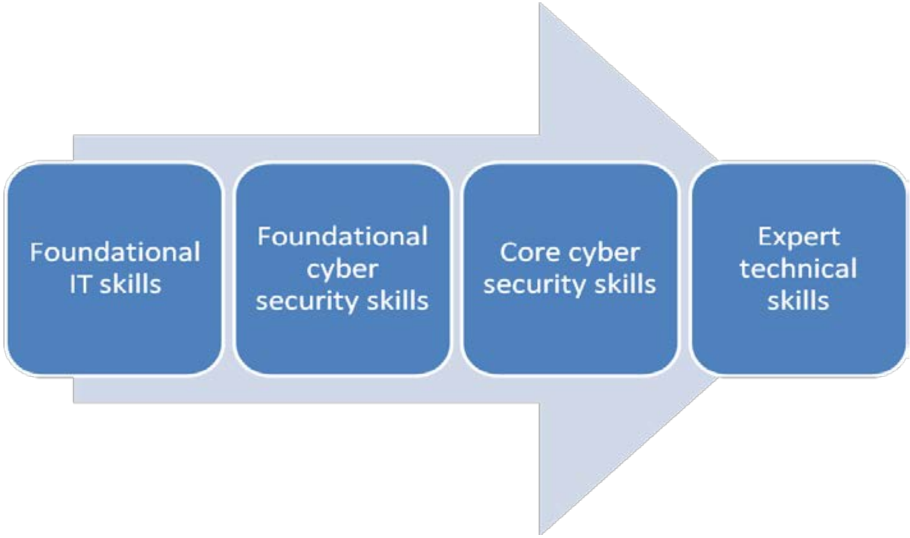
- Overview
- Training Stages
- End Game
- Schedule
- Funding Sources

Program Details

- Overview
  - Started with a small group of 20 in a pilot program
  - Use a dozen certifications
  - Use the Cyber Range
  - Use Performance Based Assessments

Program Details

- Training Stages
  - 4 stages
  - 4 quarters – 1 year



Foundational IT skills

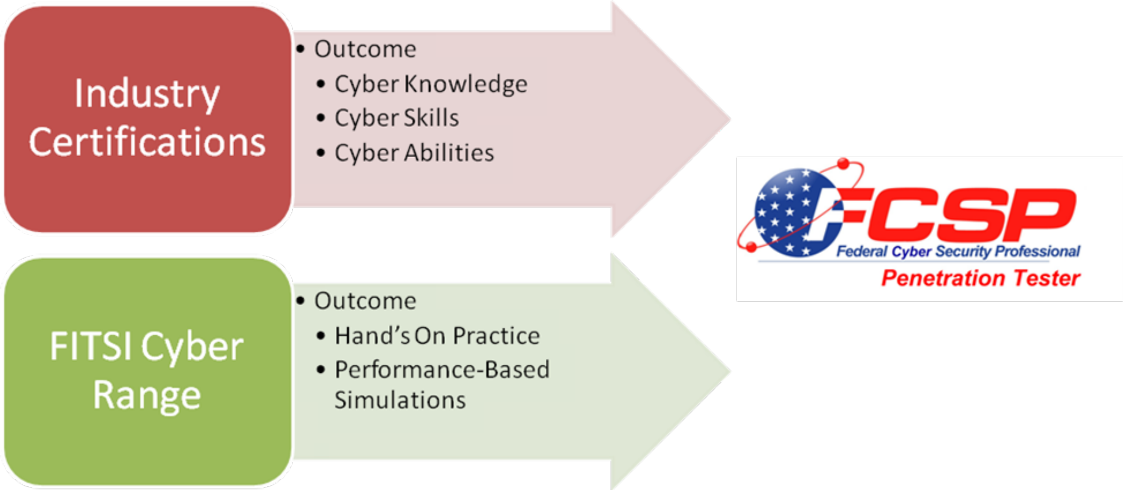
Foundational cyber security skills

Core cyber security skills

Expert technical skills

Program Details

- End Game



Industry Certifications

- Outcome
  - Cyber Knowledge
  - Cyber Skills
  - Cyber Abilities

FITSI Cyber Range

- Outcome
  - Hand's On Practice
  - Performance-Based Simulations

Program Details

- Schedule – Timing Breakdown

Program	Time Period
A+	6 Weeks
Network+	5 Weeks
Server+	5 Weeks
Linux+	5 Weeks
Security+	5 Weeks
SCNS	5 Weeks
SCNP	5 Weeks

Program Details

- Schedule – Typical Month

Sun	Mon	Tue	Wed	Thu	Fri	Sat
					1	2
3	4	5 Cyber Team Cohort (6:00-10:00pm)	6	7 Cyber Team Cohort (6:00-10:00pm)	8	9
10	11	12 Cyber Team Cohort (6:00-10:00pm)	13	14 Cyber Team Cohort (6:00-10:00pm)	15	16
17	18	19 Cyber Team Cohort (6:00-10:00pm)	20	21 Cyber Team Cohort (6:00-10:00pm)	22	23
24	25	26 Cyber Team Cohort (6:00-10:00pm)	27	28 Cyber Team Cohort (6:00-10:00pm)		

Program Details

- Funding Sources
  - Initial pilot program handled with corporate/personal sponsor donations
  - Future funding to be handled by charitable donations
    - Setup the FITSI Foundation
    - Received 501c3 status as of August 4th, 2013
      - Only took IRS application 90 days!

The Players

- Online Providers
  - Avaya Government Solutions
    - Provides the Online “Avatar-based” learning platform
  - Department of Defense
    - Provides the online cyber range

AVAYA
GOVERNMENT
SOLUTIONS

The Players

- Certification Bodies
  - CompTIA
    - Provides the entry-level certifications
  - EC-Council
    - Provides some of the highly technical certifications
  - FITSI
    - Provides the federally focused certification programs
  - ISC2
    - Provides the “core” cyber security certification programs
  - Security Certified
    - Provides the foundational cyber security certification programs

The Players

- Textbook Providers
  - Axzo Press
  - Logical Operations

Registration Process

- What traits are ideal for Wounded Warriors
- Criteria for W2CCA Registration
- How to Apply

Registration Process

- What traits are ideal for Wounded Warriors
    - Ideal candidates will possess
        - Desire to enter a market with a “zero” percent unemployment rate
        - Ability to think abstractly
        - Aptitude to work well with others
        - Geek traits as it relates to technology
        - Ability to commit to a long term program
        - Acceptance of a career requiring continuous learning

Registration Process

- Criteria for W2CCA Registration

  1. Be transitioning or have transitioned from military service;

  2. Suffer from injuries or illnesses incurred while deployed in overseas contingency operations supporting Operation Iraqi Freedom (OIF) and/or Operation Enduring Freedom (OEF) since September 11, 2001; and

  3. Receive, or expect to receive, a physical disability rating of 30% or greater in at least one of the specific categories listed below that substantially affect a major life function, or receive, or expect to receive, a combined rating equal to or greater than 50% for any other combat or combat related condition:

     - Blindness/loss of vision
     - Deafness/hearing loss
     - Fatal/incurable disease
     - Loss of limb
     - Permanent disfigurement
     - Post traumatic stress
     - Severe burns
     - Spinal cord injury/paralysis
     - Traumatic brain injury
     - Any other condition requiring extensive hospitalizations or multiple surgeries

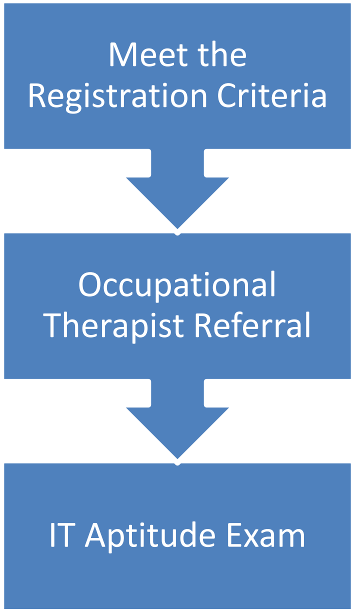
Registration Process

- Criteria for W2CCA Registration
  - Should a service member be unable to participate due to the severity of his/her injuries, the same support will be extended to a member of his/her immediate family who may be seeking training. Widows and widowers of service members who have paid the ultimate sacrifice during OIF or OEF are also eligible for support under the W2CCA program. If support is provided to a family member and the service member becomes able to participate, support will then be extended to him/her.

Registration Process

- How to Apply

Active Duty

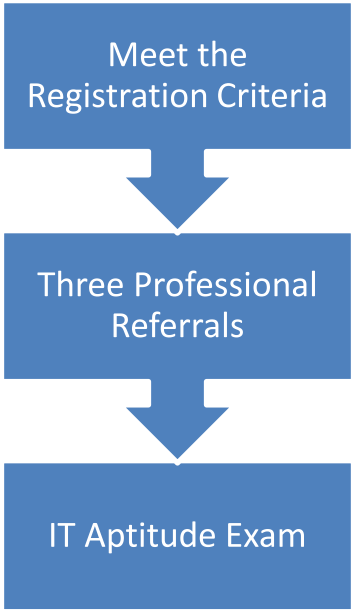


Meet the Registration Criteria

Occupational Therapist Referral

IT Aptitude Exam

Veteran



Meet the Registration Criteria

Three Professional Referrals

IT Aptitude Exam

The Results

- Program will benefit
  - The Nation
  - The League of Wounded Warriors
  - The Cybersecurity Industry

The Results

- Benefits to the Nation
  - Highly trained cyber defenders
  - Graduates will have real job performance
  - Every candidate will be fully DoD 8570 compliant in multiple levels of the Information Assurance Management (IAM) and Information Assurance Technical (IAT) certification framework

The Results

- Benefits to the League of Wounded Warriors
  - Ability to continue serving their country
  - Using their military aptitude to defend the Nation in a new theatre of battle
  - Enter a job market where there is a virtual zero percent unemployment rate*

The Results

- Benefits to the Cybersecurity Industry
  - Begin to build the necessary technical cyber capability
  - Helps address workforce shortage of personnel
  - Establishes comprehensive training framework using existing industry players

How Can You Help?

- Three ways to help
  - Recruit a wounded warrior you may know
    - Point them to http://www.w2cca.org
  - Ask your organization to become a corporate sponsor
    - Corporate sponsorship form
      - http://www.fitsi.org/w2cca-cs.pdf
    - Three levels of sponsorship
      - Gold
      - Silver
      - Bronze
  - Consider a personal donation
    - Any level of giving is greatly appreciated
    - Make a tax deductible donation to the FITSI Foundation at http://www.w2cca.org

Contact Information

- Sam Maroon
  - 703-302-3155 – maroonsa@state.gov
- Jim Wiggins
  - 703-828-1196 x701 – jim.wiggins@fitsi.org

- Wounded Warrior Cyber Combat Academy Website
  - http://www.w2cca.org
- FITSI
  - http://www.fitsi.org

Questions and Answers

- Comments?
- Questions?
- Thoughts?

Recap

- The Idea…
- Why?
- What?
- How?