Helping our Wounded Warriors and our Nation by Building Technical Cyber Capabilities

Building the Next Generation of Cyber Defenders

Wounded Warrior
Cyber Combat Academy

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

This page is left intentionally blank

TABLE OF CONTENTS

1. Executive Overview

In today's hyper connected cyber world the need for highly trained cyber defenders has never been greater. Attacks over the past several years have highlighted the perilous nature in which the nation finds itself today. Major firms such as RSA, Booz Allen and Lockheed Martin sustained serious cyber attacks over the past few years. Stuxnet and Wiki leaks became two predominant stories in 2010 and 2011. Government agencies and research laboratories (such as the Oak Ridge National Laboratory) have sustained serious attacks to their infrastructures. The dependency on information and information technology has created a double edge sword that creates both tremendous opportunities for our country as well as tremendous risk. The porous nature of technology and commerce has created an inherent risk.

Combating these threats requires more than a tool or a device. It requires a sufficient number of adequately equipped cyber defenders. For the Nation, the challenge has been to find the right type of candidate with the right skills. Today's cyber security market has evolved out of the IT industry, but influencing the IT workforce that operates the nation's IT systems to move to the cyber battlefront has not been easy. While there is serious market demand for cyber security professionals, much of it has been filled by information assurance policy and governance professionals that lack core technical skills. There is a gap.

Qualifying a cyber security professional is not an easy task. Certifications are one measurement that attempt to identify candidates but fall short in being able to assess the knowledge, skills and abilities of cyber defenders. This is not because the certifications are flawed but rather because there is no one certification that does it all. Likewise, technological innovations such as expert systems and rigorous processes are promising but do not fill the technical skills gap. The answer lies in finding, training, and certifying enough qualified cyber defenders to close shortfalls.

An intellectual resource pool that has been overlooked is the league of Wounded Warriors who are a part of the American fabric. These men and women typically hurt in combat represent an ideal group, ready to be retrained and reoriented to the cyber battlefront and deployed to help address emerging cyber threats.

This paper discusses the use of industry cyber security certifications to build the next generation of cyber defender. It is based upon bringing together the right type of candidates (wounded warriors), teaching them the right set of knowledge, skills and abilities (a comprehensive curriculum of industry standards and certifications) so they can be assessed through the use of performance based assessments.

2. The Need for Technical Cyber Defenders

In November of 2010 the Center for Strategic and International Studies (CSIS) released a white paper titled "A Human Capital Crisis in Cyber Security." While some of the recommendations in the paper were controversial and were received with mixed reaction in the cyber security market, the basic argument of the paper was correct: *Technical Proficiency Matters when it comes to Cyber Security Professionals.*

Current events continue to validate this argument. Today's cyber attacks are continuing to become more technically astute and effective. Gone are the days of simple denial of service attacks targeting websites and other internet facing IT systems. Today's attacks target the intellectual property and secrets of organizations in every industry, profession and sector of the country. The stealing of information is a common occurrence where an organization may be infiltrated from across the Internet and lose its critical secret in a very short period of time.

These insidious attacks, sometimes known as the Advanced Persistent Threat (APT), often go undetected because the organization has no capability to identify these advanced attack methods.

Real life situations have shown that organizations that employ highly technical cyber security professionals in areas such as incident response, network defense, penetration testing or forensics analysis are in the best position to identify, quarantine and remediate these advanced types of cyber threats. The differentiator isn't a device or an appliance. It's the people who are able to use judgment and analysis at a deep technical level that make the difference.

The problem for our nation is this: **we don't have enough people with the right mix of technical cyber security skills to adequately protect and defend all our information systems**. With each year that more systems are added to the Internet, the skills gap between the number of technically savvy cyber defenders and number of information systems continues to widen.

To echo the previous argument, 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."* Gosler estimated in 2010 that there were only 1,000 people in the entire United States with the sophisticated skills needed for the most demanding cyber defense tasks. To meet the computer security needs of U.S. government agencies and large corporations, he says, a force of 20,000 to 30,000 similarly skilled specialists is needed.[1]

The need is real. The supply of trained personnel is limited. Something needs to be done. That something starts with this whitepaper…

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

3. The Wounded Warrior Program

A. Who is a Wounded Warrior?

Wounded warriors are military service members who have suffered a serious life altering injury, both in combat and non-combat situations, that typically ends their ability to continue to serve on active duty as determined through normal Medical Evaluation Board/Physical Evaluation Board processes. Most are returning service men and women who have served in combat environments such as Iraq or Afghanistan. Each of the four services (Army, Navy, Air Force, and Marines) supports their wounded warriors in different ways. For example, the Army runs the U.S. Army Wounded Warrior Program (AW2), the Marines run the Wounded Warrior Regiment, the Air Force runs the Air Force Wounded Warrior Program (AFW2), and the Navy has the Safe Harbor program. The following are examples of disabilities that are used as criteria to determine wounded warrior status:

- Loss of vision/blindness
- Loss of limb
- Spinal cord injury/paralysis
- Permanent disfigurement and/or severe burns
- Traumatic brain injury
- Post traumatic stress disorder
- Mental Illness not limited to Schizophrenia/Bipolar Disorder
- Fatal/incurable disease
- Any other condition requiring extensive hospitalization or multiple surgeries

Many of them receive care at the Walter Reed National Military Medical Center in Bethesda, Maryland and are eventually honorably discharged. They attempt to reintegrate into society but options can be limited for these noble servicemen and women.

B. Why is a wounded warrior an ideal candidate as a cyber defender?

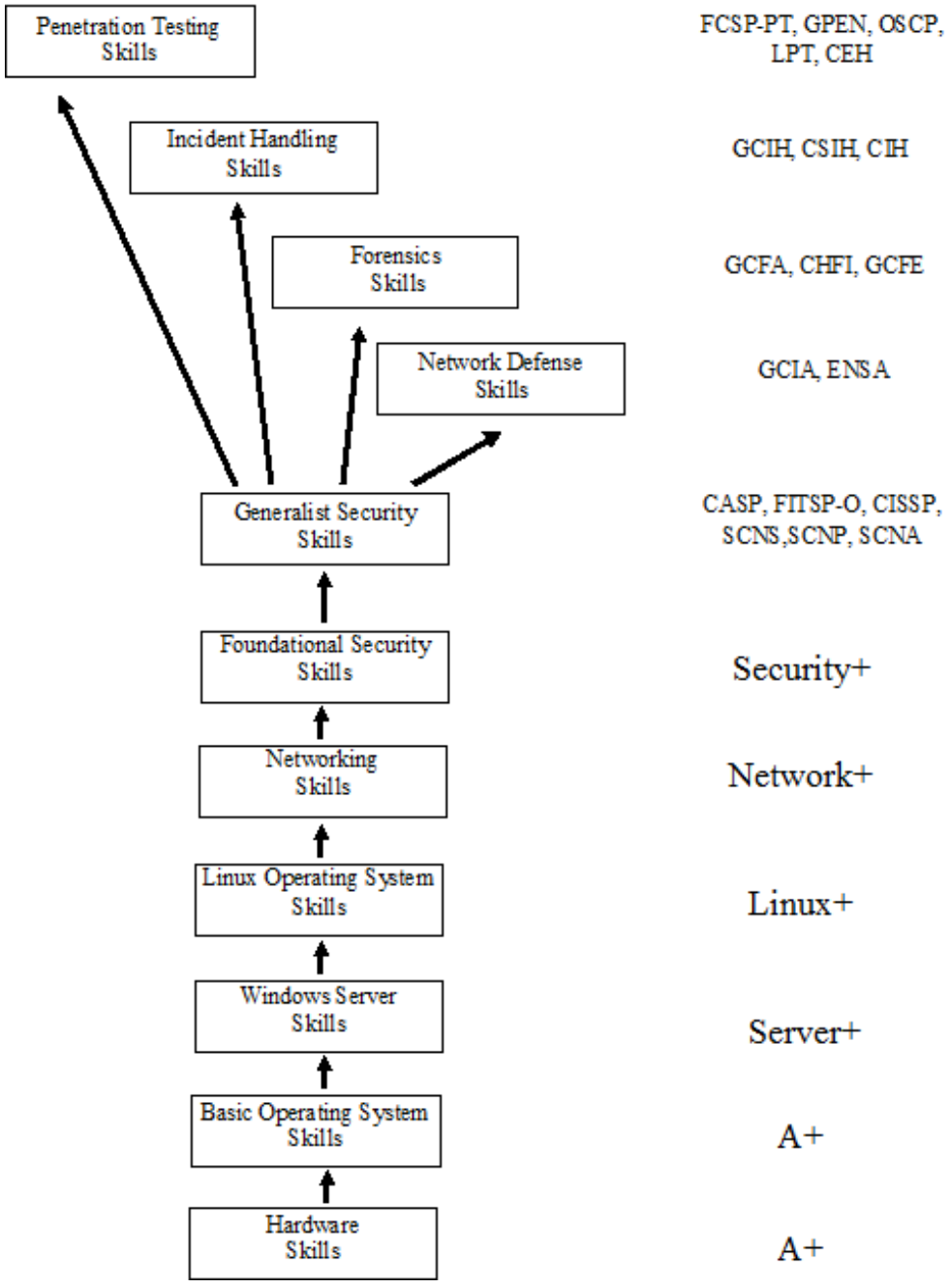
Wounded warriors are ideal candidates for a number of reasons:

1. Ability to be trained - They have demonstrated a propensity to apply themselves and be trained for highly stressful environment - physical and mental warfare.
2. Highly patriotic - They possess a high level of patriotism and desire to serve their country; they understand the need to preserve human rights and freedoms.
3. Availability of time - The nature of their injuries requires them to spend a large amount of time recovering in solitude where they could be using that time to retrain in the cyber battlefield.
4. Desire to repatriate - Becoming a cyber defender allows them to repatriate back into society in meaningful way.
5. The Nation needs them - They can help fill a critical need as the Nation needs thousands of highly trained individuals with technical cyber capabilities.
6. Aptitude for tactics and strategy – They understand physical battle tactics that correlate to the cyber battlefield.

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

4. How to Build Technical Cyber Capabilities

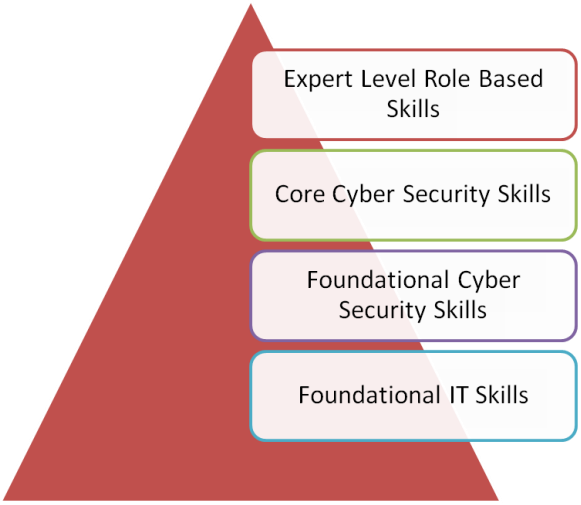
Technical cyber capabilities can be built using industry certifications in a complimentary manner. For example, below is a listing of the types of skills as shown on the left and generally associated industry certification on the right. By training for the corresponding certifications students will learn the necessary skills on the left hand side of the diagram. This model forms the basis upon which the training component discussed later is built. After completing the "General Security Skills" the candidate can pursue skills in penetration testing, incident handling, forensic skills and network defense.



5. The Approach of the Wounded Warrior Training Model

The Federal IT Security Institute has identified a comprehensive training curriculum that can take a candidate from a level of no prior knowledge up to an expert level in specialized roles such as penetration testing, security control assessment, forensics, incident handling and network defense. This approach uses a comprehensive set of industry certification programs and studies over an estimated 12 month period of time. The program can do four core things:

- Build foundational IT skills
- Build foundational IT security skills
- Build practitioner level cyber security skills
- Build expert cyber technical skills



A. Use of Industry Certifications

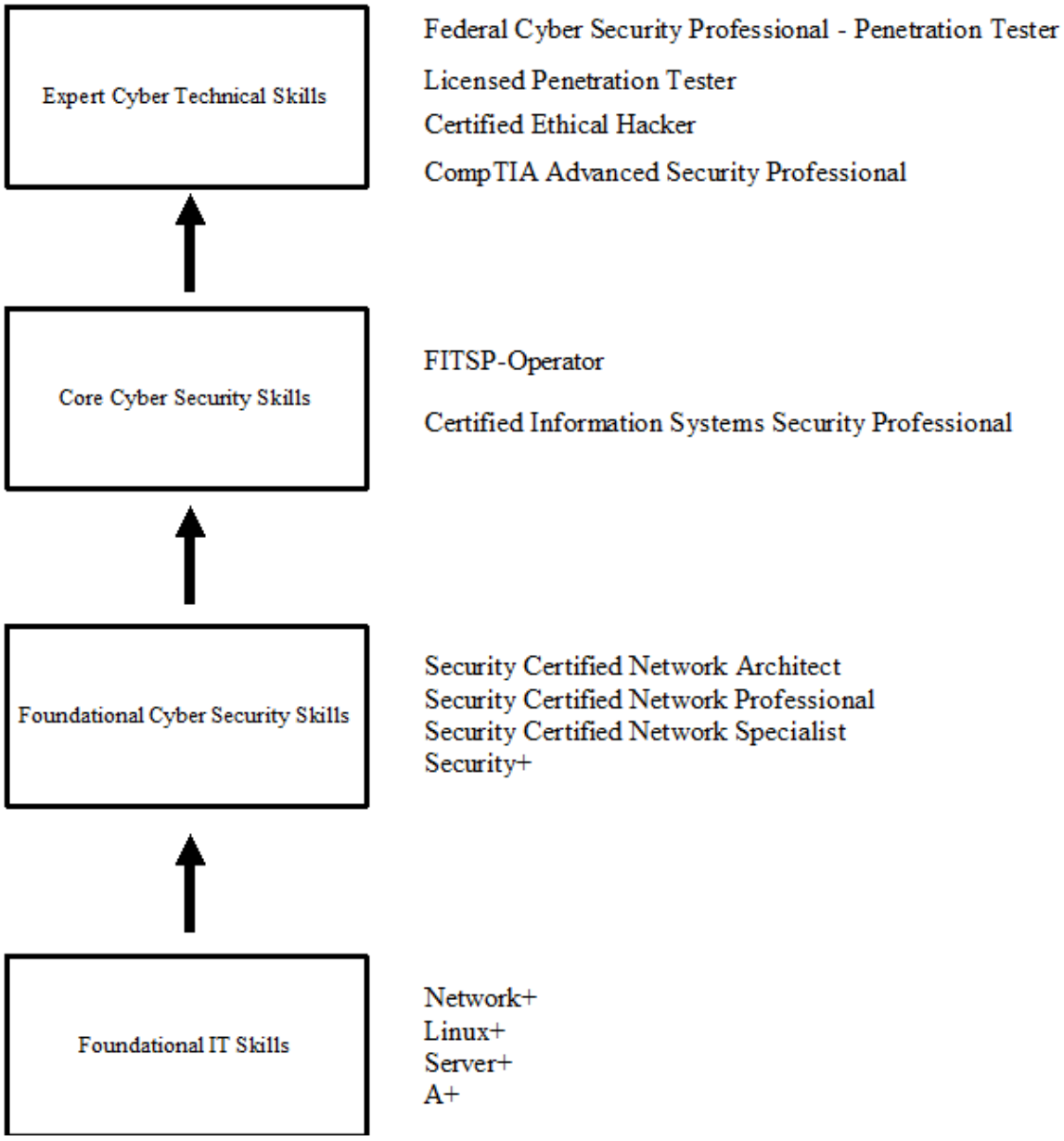
The approach uses certifications and training programs from the following certification bodies:

- CompTIA
- Ec-council
- FITSI
- ISC2
- Security Certified

Each certification body focuses on a different set of knowledge, skills and abilities as it relates to cyber security. CompTIA focuses on the foundational IT skills. Security Certified deals with the Foundational cyber security skills. ISC2 and FITSI deal with the core cyber security skills and Ec-Council deals with the highly technical cyber security abilities. When brought together these programs form a cohesive training program that works in tandem. As discussed previously, the training model provides for training

candidates in technical areas such as penetration testing, incident handling, forensic specialists and network defenders.

Below is a visual how all the certifications can work together to help build advanced cyber security skills for the penetration tester role:



B. Use of a FITSI developed Cyber Range

FITSI is planning on developing a hands-on platform for use after each certification exam has been passed so that students can continue to develop real technical skills. The purpose of this cyber range is to take the knowledge, skills and abilities obtained in the certification preparation and apply them in a hands-on environment.

The cyber range activities will bridge the certification subject matter and the performance based assessments that the subject will be required to pass to graduate from the project.

The cyber range is built based upon Federal IT security standards and mirrors the types of system configurations that the students will see both in the Federal environment and in the performance based testing. The cyber range will use case studies and scenarios to cohesively bond all the certification programs together under one framework.

Students will play in the role of member of a fictional government agency; the cyber range will be a set of 8 virtual machines loaded on laptops that the candidates will use to protect and defend. The government agency will be the Department of Cyber Security commissioned to handle the cyber security needs of the federal government. Students will begin as a help desk technician during courses such as the A+, become a network administrator, then a systems engineer and eventually transition to a security analyst. Eventually in the later courses students take on advanced technical roles that are indicative of the technical role they are pursuing. Below is a breakdown of the role of the student in the FITSI cyber range after each certification program.

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

C. Use of Performance Based Assessments

FITSI is currently developing highly focused performance based certifications known as the Federal Cyber Security Professional (FCSP). The Federal Cyber Security Professional is a role based program and is made up of five performance based certifications. They are:

1. FCSP-Penetration Tester
2. FCSP-Security Control Assessor
3. FCSP-Incident Handler
4. FCSP-Forensics Specialist
5. FCSP-Network Defender

Each FCSP certification is separate and examines a candidate's ability to demonstrate knowledge, skills, and abilities in a mock operational environment.

The FCSP exams are conducted over a two day period (Saturday and Sunday) and are broken into 3 stages. Below are the details of the three stages.

1. Multiple-choice exam - Two hour 100 question multiple choice test
The purpose of this stage is to evaluate a candidate's ability to demonstrate competency of the given job role.

2. Hands-on exam - 10 hour performance based exam consisting of 5 major tasks
The purpose of this stage is to validate that a candidate has technical competency

3. Written/Essay exam - 8 hour writing component where the candidate must create a report detailing their observations. (A template is provided to all candidates to ensure consistency). The purpose of this stage is to validate that the candidate can put together a report documenting the issues, root causes and remediation steps to be taken to fix the issues. This stage will test both the writing skills of the candidate as well as his or her ability to thinking analytically about the cause of the problem and how the organization should deal with or dealt with the situation.

6. Program Details

A. Overview

The Wounded Warrior training program is made of a dozen or more certification programs and a hands-on cyber range developed by FITSI to do two things: 1) Provide students will extensive hands-on skills and 2) Provide a learning environment for the performance based assessment which is the capstone of the project.

FITSI is planning on working with support groups to recruits a cadre of 10 candidates who have the aptitude for IT and security knowledge bases. This cadre will form the pilot program that will be lead through the program.

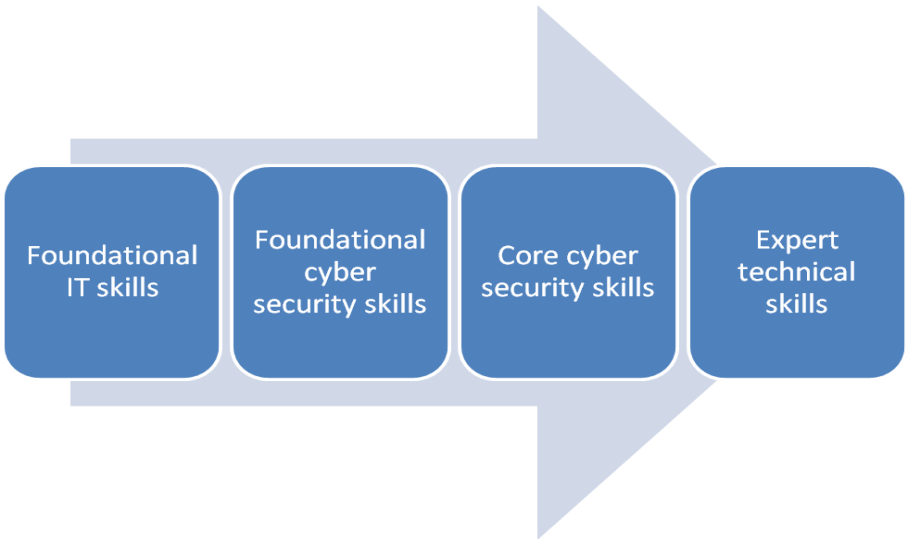
B. Training Stages

The Wounded Warrior training program will be broken down into a yearlong program (4 quarters) with the capstone project being the performance-based examination. Each quarter will focus on a different core set of knowledge, skills and abilities.

The high level overview of each quarter is listed below:

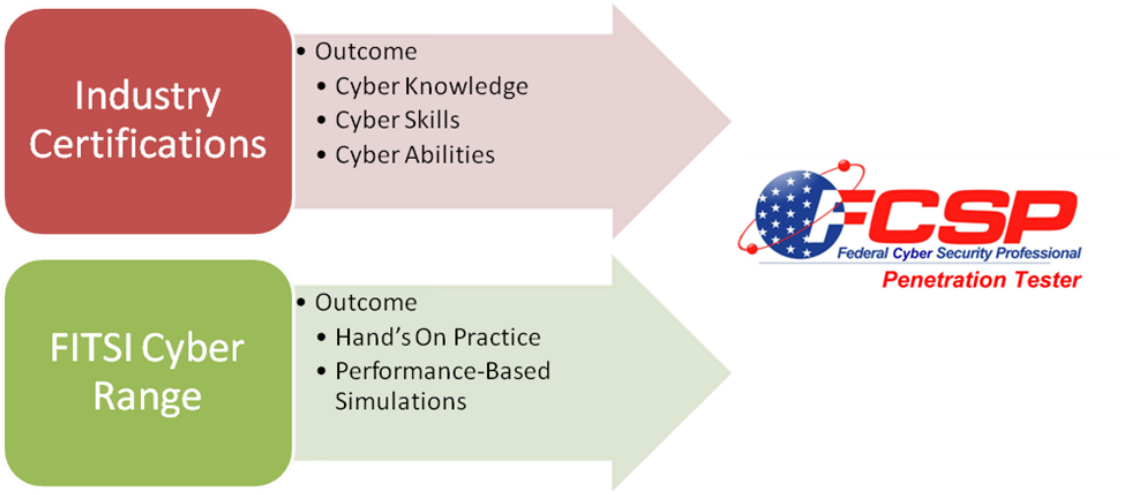
Training Quarter #1 – Foundational IT skills
Training Quarter #2 - Foundational cyber security skills
Training Quarter #3 – Core cyber security skills
Training Quarter #4 - Expert technical skills

Below is a visual of the training stages:



C. Pilot Program End Game

The pilot program will have a capstone objective that will be to obtain the FCSP-Penetration Tester certification. Having a performance based objective will cause candidates to focus on developing real hands-on technical skills during the year-long training cycle. The industry certifications will provide the knowledge, skills and abilities that the students will need to build and the FITSI cyber range will give students an opportunity to hone their skills in preparation for the performance based capstone. The visual below illustrates this idea:



D. Costs

The cost of the program will be substantial once it scales to complete fruition. Initially FITSI is seeking corporate sponsors and help from many of the certification bodies to donate textbooks and exam vouchers for the initial pilot program.

E. Funding Sources

As mentioned, during the initial pilot program we are planning on selecting a group of 10 candidates to work through the program. Donations will help finance the initial group's training. After the model has been proven, funding for the program's sustainment is needed and will be explored.

F. Schedule (Online Classes)

The planned schedule will use class sessions attended online two nights a week (Mon/Wed or Tues/Thurs) from 6:00pm to 10:00pm. Each course will be covered in a 5 week format. The students will conduct hands on lab activities offline between sessions with the instructor utilizing the Cyber Range discussed in this white paper. Below is a sample calendar of what a student's time online would look like in a given month. You will notice that A+ is highlighted in this example.

Online Class Session with Instructor

Mon	Tue	Wed	Thu	Fri
		1	2	3
6	Cyber Team Cohort A+ (6:00-10:00pm)	8	Cyber Team Cohort A+ (6:00-10:00pm)	10
13	Cyber Team Cohort A+ (6:00-10:00pm)	15	Cyber Team Cohort A+ (6:00-10:00pm)	17
20	Cyber Team Cohort A+ (6:00-10:00pm)	22	Cyber Team Cohort A+ (6:00-10:00pm)	24
27	Cyber Team Cohort A+ (6:00-10:00pm)	29	Cyber Team Cohort A+ (6:00-10:00pm)	31

The plan is to have the following certification courses to be covered during the following period:

Program	Month / Year
A+	October 2012
Server+	November 2012
Linux+	December 2012
Network+	January 2013
Security+	February 2013

SCNS	March 2013
SCNP	April 2013
SCNA	May 2013
CISSP	June 2013
FITSP-Operator	July 2013
CASP	August 2013
CEH	September 2013
LPT	October 2013
FCSP-PT	November 2013

G. Use of Avatar Based Software

A key piece of the equation is the use of an avatar based training platform known as AvayaLive Engage. This allows students to create an avatar and attend classes virtually from anywhere in the world. Using special sound technology students can carry on private or group conversations that allow collaboration and knowledge sharing between participants.

More information about this platform can be found at the following site:

http://avayalive.com/Engage/Products.aspx

Use of an avatar based platform will allow the W2CCA to reach a distributed audience. Since it is believed all Wounded Warriors have laptops they can attend the training sessions from anywhere in the world.

H. Targeted Population

While the initial targeted population is to find 10 wounded warriors as part of the pilot group, we envision the ability to service hundreds of wounded warrior once the program expands. Ideally we would like the first ground to be based out of Walter Reed but we plan on expanding the program to include those servicemen who have already been discharged and have returned home in different parts of the country.

7. The Players

A. CompTIA

CompTIA is the voice of the world's information technology (IT) industry. As a non-profit trade association advancing the global interests of IT professionals and companies, CompTIA focuses their programs on four main areas: education, certification, advocacy and philanthropy.

B. EC-Council

The International Council of E-Commerce Consultants (EC-Council) is a member-based organization that certifies individuals in various e-business and information security skills. It is the owner and creator of the world famous Certified Ethical Hacker (CEH), Computer Hacking Forensics Investigator (CHFI) and EC-Council Certified Security Analyst (ECSA)/License Penetration Tester (LPT) programs, as well as many others programs, that are offered in over 60 countries through a training network of more than 450 training partners globally.

C. FITSI

FITSI - The Federal IT Security Institute is a 501(c) (6) membership non-profit organization that is supported by exam and annual maintenance fees from its members. Founded in 2009, FITSI was established to help provide a certification scheme for federal IT security workers in the United States. Members can pursue up to four certification roles that are commonly found in Federal agencies in the United States government (Manager, Designer, Operator, Auditor).

D. ISC2

(ISC)²®, is the global, not-for-profit leader in educating and certifying information security professionals throughout their careers. They are recognized for Gold Standard certifications and world class education programs. ISC2 provides vendor-neutral education products, career services, and Gold Standard credentials to professionals in more than 135 countries. ISC2 takes pride in its reputation built on trust, integrity, and professionalism. And they're proud of their membership – an elite network of nearly 75,000 certified industry professionals worldwide.

E. Security Certified

The Security Certified Program provides the most comprehensive network security training curriculum available. SCP's certification options prepare IT professionals to combat the rapidly escalating security challenges facing IT organizations today.

8. The Results

The Nation needs a solution to the cyber security problem. The Federal IT Security Institute is building a solution to address the IT security skills gap. By tapping into the Wounded Warrior program FITSI hopes to recruit ideal candidates who can help make a difference. This work will not be easy but the outcome will have a number of benefits:

Benefits to the Nation include:

- 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

Benefits to the Wounded Warrior include:

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

*** - http://www.govinfosecurity.com/security-pros-go-full-year-no-joblessness-a-4385**

9. Program Oversight

The W2CCA program is currently overseen by group of "concerned citizens" who are interested in promoting the development of cyber defenders through the League of Wounded Warriors in the United States armed forces. 3 of the 4 four concerned citizen are former military service men who see this program as a way to help close the skills gap by leveage a pool of talent exists today but is not being tapped into.

Descriptions of these "concerned citizens" are listed below.

A. Manny Galvan, Concerned Citizen

Manny Galvan is with IBM Corporation and has over 30 years experience in information systems, logistics and financial management both in the Federal Government and private sector. He has managed system development and infrastructure projects and programs to include: SW development, data warehousing, web portal platform implementations, data center operations and maintenance (O&M), system certification and accreditations (C&A), training system requirements, project and program office enablement & operations, and system and program audits.

While in the Marine Corps, he was a supply officer. Unit assignments include 2d and 1st 8 Inch Howitzer Batteries, 4/11; 3d Tank Battalion; MAG-15; and 2d Maintenance and 2d Supply Battalions. During Desert Shield/Storm, he served as a company commander. He held operations officer and executive officer billets and has served on multiple joint-staffs. Manny has a BS in Business Administration from George Mason University and a MS in Information Management from Marymount University. Professional certifications include: PMP, CISM, and ITIL v3.

B. Sam Maroon, Concerned Citizen

Sam is an IT Operations Instructor for the US Department of State where he teaches IT Security, Security Accounting, Secure Messaging, Secure Telephony, Crypto- Key Management, Secure Radio, Classified Equipment Lifecycle and Overseas Communication Operations.

Sam was an Electronic Warfare Officer and Tactics Officer while serving in the US Air Force where he developed and taught tactics and tactics planning during the First Gulf War. He has a BS in Engineering from the Virginia Military Institute, an MBA from Rensselaer Polytechnic Institute, and a Master's Certificate in Project Management from George Washington University.

C. William Rybczynski, Concerned Citizen

William is the Vice President of the RPI Group Inc. and a founding member of the Federal IT Security Institute. Joining RPI in May 2011 as the VP of the Cyber security Division, he brings 15 plus years of cyber security technical and training experience

supporting the U.S. Department of Defense. He is professionally certified as a CISSP, CISM, NSA IAM and NSA IEM.

He also served 20 years as a United States Marine and was selected as one of the Marine Corps first Information Assurance Technicians (MOS 0689) retiring in 2006 after serving as the Information Assurance Chief, Headquarters, C4 where his responsibilities included management of the Marine Corps Information Assurance Program. Prior to joining RPI, he successfully led his previous company to a 400% sustained increase in support to the Department of the Navy's Information Assurance Workforce Improvement Program.

D. Jim Wiggins, FITSI Executive Director

Jim possesses over 16 years direct experience in the design, operation, management, and auditing of information technology systems, with the past 12 years focused on information systems security. He has an extensive background in technical education and specializes in security certification courses targeted at federal and government contracting clients.

Additionally, Jim is the executive director of the Federal IT Security Institute (FITSI). FITSI is a non-profit organization that provides a role-based IT security certification program targeted at the federal workforce. In 2011, the Federal Information Systems Security Educators' Association (FISSEA) named him "Educator of the Year" for the impact he is making in the federal workforce.

Jim holds the following IA/IT security certifications: FITSP-M, CISSP,ISSEP, CISM, CISA, SCNA, SCNP, CAP, IAM, IEM, SSCP, CEH, ECSA, CHFI, LPT, TICSA, CIWSA, Security+, and MCSE: Security.

10. Qualifications of the Trainers

The Federal IT Security Institute has a team of highly trained instructors with years of IT security, training and Federal government experience. To demonstrate the caliber of individuals that are involved in this project they are listed below with their qualifications and capabilities. All of these instructors are involved in the FITSI Wounded Warrior Project.

E. Pierre Colombel, Senior Technical Trainer

Pierre runs his own successful IT consulting business that is focused on Microsoft based cloud computing. He is a successful trainer teaching security courses for a number of clients. He is a high-energy, well-rounded senior consultant/trainer successful in overseeing the development and implementation of enterprise strategic visions through a balanced approach of skilled personnel, practical policy, well-defined procedures and tactical technology deployments. Leverages over 15 years of diverse industry experience and business acumen gained with start-up and mature multi-million dollar companies. Skilled at developing and maintaining customer relationships and identifying and exploiting opportunities

Pierre has the following IT security certifications: CISSP, ECSA, LPT, CEH, CHFI and Security+

B. Leo Dreiger, Senior Technical Trainer

Leo owns and has operated TheSecurityMatrix.com since 1995 in which he oversees the development of policies and procedures related to data protection mechanisms. Leo plans, organizes and orchestrates risk management and customer supporting non-repudiation services, determining security vulnerabilities from a variety of modern exploit tools. He is a highly skilled IT Consultant focusing on fixing hardware related problems, software upgrades and roll outs, network repair, upgrades and purchasing, wiring documentation and design. Configuration and support for Intrusion Detection Systems, ISA server, Firewalls, and Network Security. Leo has also provided consulting services to many Federal clients to include The Department of State, The Department of Labor, Internal Revenue Service and the Centers for Medicaid and Medicare, and more. Additionally, he has help thousands of IT professionals achieve their certifications and maintains an evaluation level above 90 percent.

Leo has the following IT security certifications: CISSP, CISM, CISA, CEH, CHFI, CISM, Security+ and Network+.

C. John Dunleavy, Senior Technical Trainer

John Dunleavy is the President and Founder of the Dunleavy Group an Information Technology consulting firm. John provides world class IT support training and business Information technology security consulting services. With more than 25 years' experience, John provides top of the line solutions for a broad range of clients and is considered an expert in information security, network design and problem solving by his

peers and clients. John's focuses much of his time consulting with businesses on how to protect their valuable electronic information from attack and theft, as well as lecturing and training staff at firms like Booz Allen Hamilton, TASC, Boeing, Teledyne and members of the US Armed Forces on information security related topics and certifications like CISSP (Certified Information Systems Security Professional), Security + and Certified Ethical Hacker. John is also a Microsoft Certified Trainer, and MCSE 2003 and MCITP for Windows Server 2008 and Windows 7

John has the following IT security certifications: CISSP, CEH, Network+ and Security+

D. Tyler Harding, Senior Governance Trainer

Tyler is a Principal in Kearney & Company's IT Advisory practice with over 16 years of IT experience. Tyler's expertise is in information security, particularly in the Federal government environment. He has worked as a consultant to CIOs and Office of Inspector General's of Federal agencies and advised his clients on implementing the mandatory security requirements promulgated by NIST. He currently teaches both the CISA and CGEIT review courses for the local ISACA chapter in the Washington, DC area.

Tyler has the following IT security certifications: FITSP-A, CISSP, CAP, CISA and CISM

E. Clarence Hoop, Senior Governance Trainer

Clarence worked in the Office of the Secretary of Defense at the Pentagon in various computer security positions. He retired after 40 years and by retirement he has been promoted into the Senior Executive Service. Today he teaches various certification courses to include CISSP, CE|H, and Security+. He graduated from Drexel University with a B.S. in Mathematics.

Clarence has the following IT security certifications: CISSP, Security+

F. Tina Kuligowski, Senior Technical Trainer

For over 20 years Tina has worked with information systems as a programmer for NASA, system administrator for Lexis-Nexis, curriculum developer & and systems trainer for the Department of State. She has a master's degree in information assurance, and a number of IT security certifications, to include FITSP-M, FITSP-O & FITSP-A, (ISC)2 CAP & CISSP, EC Council CEH, CEFI & DRP; in addition, she holds a number of vendor specific IT certifications from Microsoft (MCITP) and Citrix (CCEE). Since 2004, with the release of the original NIST SP800-37, she has developed and delivered a broad range of training material relating to the NIST standards and guidelines for FISMA compliance, and the implementation of information system security.

Tina has the following IT security certifications: FITSP-M, FITSP-O, FITSP-A, CISSP, CAP, CEH, CHFI, DRP, Security+, and Network+

G. Sam Maroon, Senior Technical Trainer

Sam is an IT Operations Instructor for the US Department of State where he teaches IT Security, Security Accounting, Secure Messaging, Secure Telephony, Crypto- Key Management, Secure Radio, Classified Equipment Lifecycle and Overseas Communication Operations. Sam was an Electronic Warfare Officer and Tactics Officer while serving in the US Air Force where he developed and taught tactics and tactics planning during the First Gulf War. He has a BS in Engineering from the Virginia Military Institute, an MBA from Rensselaer Polytechnic Institute, and a Master's Certificate in Project Management from George Washington University.

Sam has the following IT security certifications: CEH

H. William Matthey, Senior Technical Trainer

William has been delivering security training and consulting for over 25 years. With a formidable skill set that includes management and technical skills. William is currently working on projects worldwide to develop and manage secure Enterprise solutions utilizing Windows 7 & 08 Server Technologies and advanced MIS applications for both Microsoft Corporation and the US DOD/DOS. Having worked for the US DOD and State Department William has been delivering security training and consulting services for the US government for several years. William trains DOD 8570.1 Compliance and enjoys US Security Clearance. This involves William traveling worldwide, which takes him to some interesting places. As a presenter at Tech Ed, Deep Diver Master Class and Cyber Crimes Roadshows he continues working as a Global Security Evangelist.

William has the following IT security certifications: CISSP, CISM, CEH, CASP, Security+, Network+ and A+

I. William Rybczynski, Senior Governance Trainer

William is the Vice President of the RPI Group Inc. and a founding member of the Federal IT Security Institute. Joining RPI in May 2011 as the VP of the Cyber security Division, he brings 15 plus years of cyber security technical and training experience supporting the U.S. Department of Defense. He is professionally certified as a CISSP, CISM, NSA IAM and NSA IEM. He also served 20 years as a United States Marine and was selected as one of the Marine Corps first Information Assurance Technicians (MOS 0689) retiring in 2006 after serving as the Information Assurance Chief, Headquarters, C4 where his responsibilities included management of the Marine Corps Information Assurance Program. Prior to joining RPI, he successfully led his previous company to a 400% sustained increase in support to the Department of the Navy's Information Assurance Workforce Improvement Program.

William has the following IT security certifications: CISSP, CISM, Security+, IAM, and IEM

J. Jim Wiggins, Senior Technical Trainer

Jim Wiggins possesses over 16 years direct experience in the design, operation, management, and auditing of information technology systems, with the past 12 years focused on information systems security. He has an extensive background in technical education and specializes in security certification courses targeted at federal and government contracting clients.

Additionally, Jim is the executive director of the Federal IT Security Institute (FITSI). FITSI is a non-profit organization that provides a role-based IT security certification program targeted at the federal workforce. In 2011, the Federal Information Systems Security Educators' Association (FISSEA) named him "Educator of the Year" for the impact he is making in the federal workforce.

Jim has the following IT security certifications: FITSP-M, FITSP-O, CISSP-ISSEP, CISM, CISA, CAP, SSCP, IAM, IEM, SCNA, SCNP, SCNS, CEH, ECSA, CHFI, LPT, TICSA, CIWSA, Security+, and MCSE: Security

K. Jim Wilson, Senior Technical Trainer

Jim is an experienced Information Assurance Professional paving new trails while setting the direction, the pace, and the mind-set to find complete solutions to the most challenging problems. Jim enables humans and technologies, with fact based science to defend, secure, and counter unwanted digital activities across and throughout enterprise environments. He specializes in Electronic Countermeasures, imaginative and creative solution.

Jim has the following IT security certifications: FITSP-M, CISSP, CEH, Security+ and Network+