Veterans Cybersecurity Group- Federal Cybersecurity Professional Program

This DoD SkillBridge-approved program allows Veterans Cybersecurity Group to train, certify, mentor, and hire active-duty US Service members during the last 180 days of their enlistment. This program is offered at no cost to service members, or government the government. VCSG's return on our training investment is the development of a strong talent pipeline of TS/SCI cleared and DoD Level II Certified cybersecurity professionals.

The DoD SkillBridge program is an excellent way for service members to gain valuable skills and experience that will qualify them, through training, industry certifications, and "on-the-job" mentoring in the field of Federal Cybersecurity. Service members continue to receive their military pay and benefits while participating in the program, as they train in the VCSG Federal Cybersecurity Program.

More on the Federal Cybersecurity Professional Program

The VCSG Federal Cybersecurity Professional Program, in combination with CISSP certification, provides a solid baseline of certifications for US Service Members seeking to transition into civilian federal cybersecurity workforce. To work on a DoD network students must obtain an IAT Level III certification as required by DoD 8170 Information Assurance Level III Certification, which our ISC2 Official CISSP Boot-Camp facilitates.

> DoD work requires IAT Level III certification, which can be obtained by passing the DoD 8170 Information Assurance Level III Certification exam.
>
> ISC@'s Official CISSP Boot-Camp can help Service Members prepare for and pass both the CISSP and DoD 8170 exams.

The CISSP certification is considered the gold standard for cybersecurity professionals and is highly sought-after by employers in both the public and private sectors. The VCSG Federal Cybersecurity Professional Program provides Service Members with the training and experience they need to prepare for and pass the CISSP exam.

For DoD work, IAT Level III certification is required. The DoD 8170 Information Assurance Level III Certification is a more specialized certification focusing on cybersecurity for DoD systems and networks. ISC2's Official CISSP Boot-Camp facilitates Service Members prepare for and pass the difficult CISSP exam..

Here is a summary of the key points in your statement:

- The VCSG Federal Cybersecurity Professional Program and CISSP certification provide a solid baseline of certifications for US Service Members seeking to transition into the civilian federal cybersecurity workforce.

- VCSG Federal Cybersecurity Professional Program, with CISSP certification, provides a strong baseline for US Service Members transitioning to civilian federal cybersecurity. DoD work requires IAT Level III certification, which the DoD 8170 exam assesses. ISC2's Official CISSP Boot-Camp can help Service Members prepare for both exams.

The Federal Cybersecurity Professional Program's Four Phases

1. **Federal Baseline Phase**: includes getting accredited in Federal Cybersecurity through Certifications. This includes DoD 8570 Level III Certification (CISSP) and FISMA/NIST Accreditation via the FITSP Auditor Certification.

2. **Specialty Training Phase**: Phase two offers specialty certification and training that can be customized. Typical phase two training will include a specialty program that includes ISC2 Certification Cloud Security Professional (CCSP), FITSP-Auditor Certification, CMMC Register Practitioners, (RP), and Certified Assessors (CCAs).

3. **Zero Trust Phase:** Phase three provides training in Zero Trust principles and Agile AI/ML deployment as part of a Security Operations, and development Team, or (SecDevOps)

4. **Phase Four Job Placement Phase,** the final phase is the continuation of VCSG efforts to place each separating Service Member into the civilian cybersecurity workforce. This may include further specialty training and certification as per the requirements specified in the

Federal Cybersecurity Professional Program Curriculum

Curriculum for all Service Members includes what is required for a federal position that requires CISSP, or DoD IAT8570 Level 3 certification requirements and NIST/FISMA accreditation. Later phases address specialty certification and training on Zero Trust Networking Principles and Architectures.

Phase One. Federal Cybersecurity Baseline Accreditation (Weeks 1 through 5)

1. DoD 8570 IAT Level III Certification via our CISSP Program
2. FISMA/NIST Accreditation through the FITSP (Federal IT Security Professional) Auditor certification.

Week 1: Federal Cybersecurity Program Orientation

1. Students will be introduced to the Federal Information Cybersecurity Program and the elements of their specific training plan.
2. Students will be matched with a placement counselor to evaluate current military experience, training, and security clearance and match it to a crafted training program that meets the requirements of current federal cybersecurity positions.
3. Service members are introduced to the CISSP Common Body of Knowledge(CBK). The (ISC)² CBK is a collection of topics relevant to cybersecurity professionals worldwide.
4. CISSP Module One: Introduction to Security and Risk Management
5. CISSP Domain Two: Asset Security

Week 2: CISSP Training

1. Security Architecture and Engineering
2. Communication and Network Security
3. Identity and Access Management (IAM)

Week 3: CISSP Training

1. Security Assessment and Testing
2. Security Operations
3. Software Development Security

Week 4: CISSP Domain Review and Exam Prep

Week 5: Federal Cybersecurity Law and Standards

1. Understanding the Federal Information Security Management Act of 2002 (FISMA)
2. Applying the required National Institute of Standards (NIST) to federal information systems
3. Risk Management Framework for Information Systems and Organizations
4. Managing Information Security Risk: Organization, Mission, and Information System View
5. Conducting Risk Assessments
6. Security and Privacy Controls for Information Systems and Organizations

Phase Two: Specialty Certifications and Training

Week 6: Cloud Security

1. Certificate of Cloud Security Knowledge (CCSK)
2. CCSP | Certified Cloud Security Professional

Week 7: Certified CMMC Professional

1. CMMC-AB Code of Professional Conduct
2. Registered Practitioner (RP) with basic training on the CMMC standard

Week 8: Certified CMMC Assessor Level 1-3

1. Obtain Credentials to conduct CMMC ML-1 assessments
2. Authorized to supervise Certified CMMC Professionals in ML-1 assessments.
3. Listed in the CMMC-AB Marketplace

Week 9 thru Week 12:

Mentor Led Federal Cybersecurity Engagement

- The mentor will lead service members through completing designated federal cybersecurity engagement. This may include: CMMC Assessment and Consulting, and/or Federal Agency FISMA Support

Weeks 13-20: Zero Trust Networking Modernization

1. The History and Federal Mandates that require Zero Trust
2. Introduction to Zero Trust Principles
3. Understanding FICAM: Federal Identity & Credential Management relating to Zero Trust Principles
4. Artificial Intelligence and Machine Learning in a Zero Trust Network Architecture (ZT AI/ML)
5. Security, Development, and Operations as an agile method to deploy a ZTNA (SecDevOps)
6. Introduction to SecDevOps and Agile Principles
7. The role of SecDevOps in implementing Zero Trust AI/ML Solutions utilizing Agile Principles in an Agency's System Development Life Cycle (SDLC)
8. Zero Trust Metrics including Key Progress Indicators (KPI's), and other Project Objectives
9. Incorporating continuous authentication, authorization, and monitoring of the ZTNA

*Only after achieving the objectives of the Baseline Certification Phase do students move on to the specialty Phases. Extra time is allocated to individual Tudor service members through these significant Baseline Certifications when required.

Weeks 20-26 (If available)

The remaining weeks of the the 180-day program include any specific additional, training, certification, and/or mentoring required to qualify for a specific cybersecurity position as defined by a specific federal contract being fulfilled by VCSG as a Prime, or Sub-contracting partner.