CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF INFORMATION TECHNOLOGY

Centers for Medicare & Medicaid Services
Information Security and Privacy Group

(Cybersecurity Veterans Internship Program)

CyberVets

Transitioning warfighters to civilian missions that help protect and strengthen our federal IT infrastructure

The CMS CyberVet program provides an amazing opportunity for motivated, driven and energetic veterans with little or no prior cybersecurity experience and can provide a boot in the door to the in-demand career field of cybersecurity.

Training length: 6 Months

Location: Windsor Mill, MD

Schedule: M-F, 8-4

Experience: No cyber experience required

Acceptance depends on aptitude, motivation, and commitment

If accepted, you will serve on a six-month rotation at CMS where they will engage in both authentic problem-based and “on the job” training, learning the skills required to protect our data and network. You will be mentored by staff within the Information Security & Privacy Group while developing strong working relationships by networking with all ISPG’s staff who comprise our cyber defense. Additionally, you will learn to speak the same language as CMS and other federal agency security staffs and will be able to represent security and privacy interests to business owners and management.

Upon successful completion you will be:

- Trained in cybersecurity operations, compliance, and policy
- GIAC Security Essentials (GSEC) certified
- Mentored in the CMS work environment and culture
- Have an established network and relationships among operators, cyber risk advisors, ISSOs, and management within CMS and beyond

CyberVets is a six-month program for transitioning veterans who are interested in making a career in federal cybersecurity. It is based on a proven cognitive apprenticeship problem-based learning model that prepares you to solve real problems in real contexts using real tools. It leverages the National Initiative for Cybersecurity Education Framework with attained KSAs (knowledge, skills, and abilities) aligned to work roles including those of Cyber Defense Analyst and Information Systems Security Officer/Manager.

The program is open to all interested applicants regardless of prior career field or experience.

In Summer 2020 (watch for actual date), four successful applicants will begin the program with the addition of two additional successful applicants integrated into the program at eight-week intervals. This facilitates cooperative and collaborative problem solving as the new learners are integrated into the problem-solving framework.

Goals of the program:

1. Preparation to enter cybersecurity workforce positions in civilian government services
2. Attain the knowledge, skills, and abilities (KSAs) for cybersecurity and privacy principles based on appropriate National Institute for Cyber Education (NICE) Work Roles
3. Use data collected from a variety of cyber defense tools (e.g., alerts, firewalls, network traffic logs) to analyze events that occur within their environments to mitigate threats
4. Understand and be able to help perform the activities required to support information system security processes and procedures
5. Gain confidence and expertise in communicating problems, solutions, status and project attributes at multiple levels (i.e., technical, peer, executive)
6. Provide the basic and intermediate learning foundations to begin and build a successful career in cybersecurity.

Areas of learning:

The program begins with a solid foundation in networking fundamentals and network security essentials and will progress into more advanced areas such as reverse engineering, threat management, policy, and compliance management. Candidates will develop the skills and confidence necessary for exploring modern cybersecurity theories thru hands-on learning experiences and to communicate threat status to senior leadership. Candidates will also be trained in the following but not limited areas:

- Critical thinking and problem solving
- Researching cyber security methods and trends
- Networking Essentials (foundations to advanced)
- Windows and Linux Security Essentials
- Networking Vulnerabilities
- Reverse Engineering
- Networking and analysis tools
- Defense-in-Depth Strategies
- Threat Management, Risk Management and Response
- Continuous Diagnostics and Mitigation (CDM)
- Forensics, Malware, and Analysis
- Penetration Testing Basics
- Risk management and oversight

Program Expectations:

Application and selection process:

1. Applicants will be chosen by the following:
   a. Resume
   b. Interview
   c. Aptitude (non-cybersecurity specific), motivation, and commitment
   d. Problem solving ability

Training methodologies:

1. The course is a cognitive apprenticeship problem-based learning model that will prepare you to solve real problems in real contexts using real tools.
2. Course work will be 80% hands-on learning. Candidates will learn mostly through problem solving scenarios. Candidates will learn and develop their own research and learning skills to apply to these scenarios. Teach you to teach yourself.
3. Candidates will have multiple mentors to amplify and enhance learning objectives.

Administrative:

1. Course will be Monday-Friday, 8am-4pm, with the exception of holidays.
2. Attire for the program will be casual and according to the CMS dress policy)
3. In order to maximize program and learning effectiveness, candidates are expected to be present throughout the six-month program. The course will have administrative days built into it so allow candidates to take care of necessary appointment and out-processing duties.
4. The program will have multiple check points throughout the course to assess the apprentice's performance and aptitude. If the apprentice is not meeting expectations, they will be counseled on performance. If the apprentice does not meet standards but each checkpoint, they will be removed from the program.

Course Outline

Week Number	Domain	Topic
Pre course	Admission	Application process
0	Orientation/Pre-test	Onboarding and Pre-testing
1	Operations	Intro to Security Operations Center (SOC) Analytical Methods, Networks and Virtual Machines
2	Operations	Intro to SOC Analytical Methods, Ports, OS Fingerprinting
3	Operations	Intro to SOC Analytical Methods, reverse engineering methods, tools, programming languages
4	Operations	Intro to SOC Analytical Methods, Exec Communications
5	Operations	Linux Security Essentials/Applied Network Security
6	Operations	SOC Tools and Tour

7	Policy/Compliance	Intro to information systems security officer role (ISSO) and appropriate policy
8	Compliance	Intro to CFACTS
9	Operations	Access Controls, Security Architecture, Risk Management, CMSSOC Tools, Signatures
10	Operations	SANS SEC 401 Network Security Essentials
11	Operations	SANS SEC 401 Defense-in-Depth and Attacks
12	Operations	SANS SEC 401 Threat Management
13	Operations	Network Security Advanced/ Windows Enterprise Security
14	Policy/Compliance	Advanced CFACTS - Reporting
15	Policy/Compliance	ISSO/ISSM Concepts and processes – Assessments/Audits
16	Operations	Vulnerability Analysis Tools (VAT)

17	Operations	Forensics, Malware Analysis, Tools
18	Operations	Penetration Testing
19	Operations	SANS SEC 401 Cryptography, Risk Management, and Response
20	Operations	SANS SEC 401 Windows Security
21	Operations	SANS SEC 401 Linux Security
22	Policy/Compliance	Intro to Cyber Risk Advisor, Expiring Authorization to Operate Scenario/Executive Communication
23	Policy/Compliance	Intro to Cyber Risk Advisor, Expiring Authorization to Operate Scenario/Executive Communication GSEC Scheduling
24	Out-processing/Testing	Out-processing Post-testing GSEC