

## **DESCRIPTION OF SERVICES**

The Department of Veterans Affairs (VA), Office of Information and Technology (OI&T), Quality, Privacy & Risk (QPR) requires Information Technology (IT) security training.

### **GENERAL REQUIREMENTS**

The Contractor shall provide the specific deliverables as authorized by the Contracting Officer's Representative (COR). The below requirements are common to all deliverables:

1. Virtual, online, self-paced training. Courses must be delivered in an on-line environment, accessible through the internet at any time (24/7) using a personal or government computer with a MS Windows 7 or newer operating system.
2. Credit. Courses must be eligible for Continuing Education Unit (CEU) and/or Continuing Professional Education (CPE) credit by an Information Security Industry professional certification authority listed by the National Initiative for Cybersecurity Education (NICE) (<http://niccs.us-cert.gov/training/professional-certifications>).
3. Exercises/Labs. Courses must include exercises and/or labs that facilitate student practical application of learned techniques and skills.
4. Instructor Interaction. Certified course Instructors must be available to answer student questions and to provide additional guidance as may be requested by the student. Availability may be via e-mail, instant messenger or phone. Instructor assistance must be provided no later than two business days after student request.
5. Currency of Information. IT security is a quickly evolving industry. Courses must have been reviewed and certified to be current with the last two years.
6. Certification. Course completion certificates will be issued to each student who successfully meets course completion requirements. Certificates will be issued to, or made available for download by the student within five business days of course completion.

## **PLACE OF PERFORMANCE**

No contractor work will be provided at a Government site. Coursework is accessed online via internet. Additional reference material may be provided via shipping service as required to support training curriculum.

## **METHOD AND DISTRIBUTION OF DELIVERABLES**

The Contractor shall deliver courses in an on-line environment, accessible through the internet at any time (24/7) using a personal or government computer with a MS Windows 7 or newer operating system.

### **PERFORMANCE PERIOD**

This is a one-time purchase of virtual, online, self-paced training courses. The Student access to these courses is expected to cover a period of 120 days from date of registration (i.e., the student will have 120 days to complete an individual course).

The Contractor shall deliver courses upon COR authorization and subsequent individual student course enrollment in the vendor's enrollment system; however, delivery of all courses must begin no later than July 15, 2017. The Course Registration Confirmation shall be sent to the COR within 8 hours of student's enrollment and updated after each enrollment.

**COURSE TITLES:** The following courses are offered by Sans Institute. Please submit your course information and content that matches or is similar to each of the 11 courses described below. Submit any other pertinent information that would help analyze your course contents. The scope of this purchase is a total of 18 seats split up amongst 11 course titles as follows:

Task	Description
SEC 501	<p><b>Title:</b> Advanced Security Essentials - Enterprise Defender with NetWars: Continuous  <b>Format:</b> Virtual, online, self-paced training  <b>Study Time:</b> 70 Hours  <b>Awarded CPEs/CEUs:</b> 35-40  <b>Quantity:</b> 1  <b>Delivery:</b> Within two business days after notification by COR of student identification</p> <p><b>Course Contents/Objectives:</b></p> <ul style="list-style-type: none"> <li>•Identify network security threats against infrastructure and build defensible networks that minimize the impact of attacks</li> <li>•Access tools that can be used to analyze a network to prevent attacks and detect the adversary</li> <li>•Decode and analyze packets using various tools to identify anomalies and improve network defenses</li> <li>•Understand how the adversary compromises systems and how to respond to attacks</li> <li>•Perform penetration testing against an organization to determine vulnerabilities and points of compromise</li> <li>•Apply the six-step incident handling process</li> <li>•Use various tools to identify and remediate malware across your organization</li> <li>•Create a data classification program and deploy data-loss-prevention solutions at both a host and network level.</li> <li>•NetWars Continuous Online Range Topics: Vulnerability Assessment, Packet Analysis, Penetration Testing, System Hardening, Malware Analysis, Digital Forensics and Incident Response</li> </ul>
SEC 504	<p><b>Title:</b> Hacker Tools, Techniques, Exploits, and Incident Handling  <b>Format:</b> Virtual, online, self-paced training  <b>Study Time:</b> 60 Hours  <b>Awarded CPEs/CEUs:</b> 35-40</p>

Task	Description
	<p><b>Quantity:</b> 1</p> <p><b>Delivery:</b> Within two business days after notification by COR of student identification</p> <p><b>Course Contents/Objectives:</b></p> <ul style="list-style-type: none"> <li>•Apply incident handling processes-including preparation, identification, containment, eradication, and recovery-to protect enterprise environments</li> <li>•Analyze the structure of common attack techniques in order to evaluate an attacker's spread through a system and network, anticipating and thwarting further attacker activity</li> <li>•Utilize tools and evidence to determine the kind of malware used in an attack, including rootkits, backdoors, and Trojan horses, choosing appropriate defenses and response tactics for each</li> <li>•Use built-in command-line tools such as Windows tasklist, wmic, and reg, as well as Linux netstat, ps, and lsof to detect an attacker's presence on a machine</li> <li>•Analyze router and system ARP tables along with switch CAM tables to track an attacker's activity through a network and identify a suspect</li> <li>•Use memory dumps and memory analysis tools to determine an attacker's activities on a machine, the malware installed, and other machines the attacker used as pivot points across the network</li> <li>•Gain access to a target machine using Metasploit, and then detecting the artifacts and impact of exploitation through process, file, memory, and log analysis</li> <li>•Analyze a system to see how attackers use the malware to move files, create backdoors, and build relays through a target environment</li> <li>•Run the Nmap port scanner and Nessus vulnerability scanner to find openings on target systems, and apply tools such as tcpdump and netstat to detect and analyze the impact of the scanning activity</li> <li>•Apply the tcpdump sniffer to analyze network traffic generated by a covert backdoor to determine an attacker's tactics</li> <li>•Employ the netstat and lsof tools to diagnose specific types of traffic-flooding denial-of-service techniques, and choose appropriate response actions based on each attacker's flood technique</li> <li>•Analyze shell history files to find compromised machines, attacker-controlled accounts, sniffers, and backdoors</li> </ul>

Task	Description
ICS 410	<p> <b>Title:</b> ICS/SCADA Security Essentials  <b>Format:</b> Virtual, online, self-paced training  <b>Study Time:</b> 50 Hours  <b>Awarded CPEs/CEUs:</b> 30-35  <b>Quantity:</b> 2  <b>Delivery:</b> Within two business days after notification by COR of student identification </p> <p><b>Course Contents/Objectives:</b></p> <ul style="list-style-type: none"> <li>•Run Windows command line tools to analyze the system looking for high-risk items</li> <li>•Run Linux command line tools (ps, ls, netstat, ect) and basic scripting to automate the running of programs to perform continuous monitoring of various tools</li> <li>•Install VMWare and create virtual machines to create a virtual lab to test and evaluate tools/security of systems</li> <li>•Better understand various industrial control systems and their purpose, application, function, and dependencies on network IP and industrial communications</li> <li>•Work with operating systems (system administration concepts for Unix/Linux and/or Windows operating systems)</li> <li>•Work with network infrastructure design (network architecture concepts, including topology, protocols, and components)</li> <li>•Better understand the systems' security lifecycle</li> <li>•Better understand information assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation)</li> <li>•Use your skills in computer network defense (detecting host and network-based intrusions via intrusion detection technologies)</li> <li>•Implement incident response and handling methodologies</li> </ul>
SEC 566	<p> <b>Title:</b> Implementing and Auditing the Critical Security Controls  <b>Format:</b> Virtual, online, self-paced training  <b>Study Time:</b> 60 Hours  <b>Awarded CPEs/CEUs:</b> 30-40  <b>Quantity:</b> 2  <b>Delivery:</b> Within two business days after notification by COR of student identification </p>

Task	Description
	<p><b>Course Contents/Objectives:</b></p> <ul style="list-style-type: none"> <li>•Apply a security framework based on actual threats that is measurable, scalable, and reliable in stop- ping known attacks and protecting organizations' important information and systems</li> <li>•Understand the importance of each control, how it is compromised if ignored, and explain the defensive goals that result in quick wins and increased visibility of network and systems</li> <li>•Identify and utilize tools that implement controls through automation</li> <li>•Learn how to create a scoring tool for measuring the effectiveness of each controls the effectiveness of each control</li> <li>•Employ specific metrics to establish a baseline and measure the effectiveness of security controls</li> <li>•Understand how critical controls map to standards such as NIST 800-53, ISO 27002, the Australian Top 35, and more</li> <li>•Audit each of the critical security controls, with specific, proven templates, checklists, and scripts provided to facilitate the audit process</li> </ul>
MGT 525	<p><b>Title:</b> IT Project Management, Effective Communication, and PMP® Exam Prep  <b>Format:</b> Virtual, online, self-paced training  <b>Study Time:</b> 60 Hours  <b>Awarded CPEs/CEUs:</b> 35-40  <b>Quantity:</b> 2  <b>Delivery:</b> Within two business days after notification by COR of student identification</p> <p><b>Course Contents/Objectives:</b></p> <ul style="list-style-type: none"> <li>•Recognize the top failure mechanisms related to IT and infosec projects, so that your projects can avoid common pitfalls</li> <li>•Create a project charter which defines the project sponsor and stakeholder involvement</li> <li>•Document project requirements and create requirements traceability matrix to track changes throughout the project lifecycle</li> <li>•Clearly define the scope os a project in terms of cost, schedule and technical deliverables</li> </ul>

Task	Description
	<ul style="list-style-type: none"> <li>•Create a work breakdown structure defining work packages, project deliverables and acceptance criteria</li> <li>•Develop a detailed project schedule, including critical path tasks and milestones</li> <li>•Develop a detailed project budget including cost baselines and tracking mechanisms</li> <li>•Develop planned and earned value metrics for your project deliverables and automate reporting functions</li> <li>•Effectively manage conflict situations and build communication skills with your project team</li> <li>•Document project risks in terms of probability and impact, assign triggers and risk response responsibilities</li> <li>•Create project earned value baselines and project schedule and cost forecasts</li> </ul>
MGT 514	<p> <b>Title:</b> IT Security Strategic Planning, Policy and Leadership  <b>Format:</b> On-Demand/Virtual Self-Study  <b>Study Time:</b> 50 Hours  <b>Awarded CPEs/CEUs:</b> 30-40  <b>Quantity:</b> 5  <b>Delivery:</b> Within two business days after notification by COR of student identification         </p> <p><b>Course Objectives:</b></p> <ul style="list-style-type: none"> <li>•Calculate the half-life of information</li> <li>•Establish a strategic planning horizon appropriate for your organization</li> <li>•Conduct any of the well-known environmental scans ( SWOT, Porters 5, Pest and many others )</li> <li>•Facilitate out of the box thinking (brainstorming, reverse brainstorming, synergetics)</li> <li>•Select between candidate initiatives and preform ""back of the envelope"" planning</li> <li>•Understand how policy is used and when it is needed or not needed</li> <li>•Manage the policy creation process</li> <li>•Develop policy for difficult topics such as social media</li> </ul>

Task	Description
	<ul style="list-style-type: none"> <li>•Evaluate policy using the SMART methodology</li> <li>•Understand the use of leadership competencies in developing leadership skills</li> <li>•Select a few competencies to work on to further your effectiveness</li> </ul>
SEC 575	<p> <b>Title:</b> Mobile Device Security and Ethical Hacking  <b>Format:</b> Virtual, online, self-paced training  <b>Study Time:</b> 60 Hours  <b>Awarded CPEs/CEUs:</b> 35-40  <b>Quantity:</b> 1  <b>Delivery:</b> Within two business days after notification by COR of student identification         </p> <p><b>Course Contents/Objectives:</b></p> <ul style="list-style-type: none"> <li>•Use jailbreak tools for Apple iOS and Android systems</li> <li>•Conduct an analysis of iOS and Android file system data to plunder compromised devices and extract sensitive mobile device use information</li> <li>•Analyze Apple iOS and Android applications with reverse-engineering tools</li> <li>•Change the functionality of Android and iOS apps to defeat anti-jailbreaking or circumvent in-app purchase requirements</li> <li>•Conduct an automated security assessment of mobile applications</li> <li>•Use wireless network analysis tools to identify and exploit wireless networks used by mobile devices</li> <li>•Intercept and manipulate mobile device network activity</li> <li>•Leverage mobile-device-specific exploit frameworks to gain unauthorized access to target devices</li> <li>•Manipulate the behavior of mobile applications to bypass security restrictions</li> </ul>
SEC 560	<p> <b>Title:</b> Network Penetration Testing and Ethical Hacking  <b>Format:</b> Virtual, online, self-paced training  <b>Study Time:</b> 60 Hours  <b>Awarded CPEs/CEUs:</b> 35-40  <b>Quantity:</b> 1  <b>Delivery:</b> Within two business days after notification by COR of student identification         </p>

Task	Description
	<p><b>Course Contents/Objectives:</b></p> <ul style="list-style-type: none"> <li>•Develop tailored scoping and rules of engagement for penetration testing projects to ensure the work is focused, well defined and conducted in a safe manner</li> <li>•Conduct detailed reconnaissance using document metadata, search engines and other publicly available information sources to build a technical and organizational understanding of the target environment</li> <li>•Utilize the Nmap scanning tool to conduct comprehensive network sweeps, port scans, Operating System fingerprinting and version scanning to develop a map of target environments</li> <li>•Choose and properly execute Nmap Scripting Engine scripts to extract detailed information from target systems</li> <li>•Configure and launch the Nessus vulnerability scanner so that it discovers vulnerabilities through both authenticated and unauthenticated scans in a safe manner, and customize the output from such tools to represent the business risk to the organization</li> <li>•Analyze the output of scanning tools to manually verify findings and perform false positive reduction using Netcat and the Scapy packet crafting tools</li> <li>•Utilize the Windows and Linux command lines to plunder target systems for vital information that can further overall penetration test progress, establish pivots for deeper compromise and help determine business risks</li> <li>•Configure the Metasploit exploitation tool to scan, exploit and then pivot through a target environment in-depth</li> <li>•Conduct comprehensive password attacks against an environment, including automated password guessing (while avoiding account lockout), traditional password cracking, rainbow table password cracking and pass-the-hash attacks</li> <li>•Launch web application vulnerability scanners such as ZAP and then manually exploit Cross-Site Request Forgery, Cross-Site Scripting, Command Injection and SQL injection attacks to determine the business risks faced by an organization</li> </ul>

Task	Description
SEC 506	<p> <b>Title:</b> Securing Linux/Unix  <b>Format:</b> Virtual, online, self-paced training  <b>Study Time:</b> 60 Hours  <b>Awarded CPEs/CEUs:</b> 35-40  <b>Quantity:</b> 1  <b>Delivery:</b> Within two business days after notification by COR of student identification </p> <p><b>Course Contents/Objectives:</b></p> <ul style="list-style-type: none"> <li>•Significantly reduce the number of vulnerabilities in the average Linux/Unix system by disabling unnecessary services.</li> <li>•Protect your systems from buffer overflows, denial-of-service, and physical access attacks by leveraging OS configuration settings.</li> <li>•Configure host-based firewalls to block attacks from outside.</li> <li>•Deploy SSH to protect administrative sessions, and leverage SSH functionality to securely automate routine administrative tasks.</li> <li>•Use sudo to control and monitor administrative access.</li> <li>•Create a centralized logging infrastructure with Syslog-NG, and deploy log monitoring tools to scan for significant events</li> <li>•Use SELinux to effectively isolate compromised applications from harming other system services.</li> <li>•Securely configure common Internet-facing applications such as Apache and BIND.</li> <li>•Investigate compromised Linux/Unix systems with Sleuthkit, Isof, and other open-source tools.</li> <li>•Understand attacker rootkits and how to detect them with AIDE and rkhunter/chkrootkit.</li> </ul>
SEC 505	<p> <b>Title:</b> Securing Windows and PowerShell Automation  <b>Format:</b> On-Demand/Virtual Self-Study  <b>Study Time:</b> 60 Hours  <b>Awarded CPEs/CEUs:</b> 30-40  <b>Quantity:</b> 1  <b>Delivery:</b> Within two business days after notification by COR of student identification </p> <p><b>Course Objectives:</b></p>

Task	Description
	<ul style="list-style-type: none"> <li>•Execute PowerShell commands on remote systems and begin to write your own PowerShell scripts.</li> <li>•Harden PowerShell itself against abuse, and enable transcription logging.</li> <li>•Use Group Policy to execute PowerShell scripts on an almost unlimited number of hosts, while using Group Policy Object permissions, organizational units, and Windows Management Instrumentation (WMI) to target just the systems that need the scripts run.</li> <li>•Use PowerShell Desired State Configuration (DSC) and Server Manager scripting for the sake of SecOps/DevOps automation of server hardening.</li> <li>•Assuming a breach will occur, use Group Policy and PowerShell to grant administrative privileges in a way that reduces the harm if an attack succeeds.</li> <li>•Configure PowerShell remoting to use Just Enough Admin (JEA) policies to create a Windows version of Linux sudo and setuid root.</li> <li>•Configure mitigations against attacks such as pass-the-hash, Kerberos golden tickets, Remote Desktop Protocol (RDP) man-in-the-middle, Security Access Token abuse, and others.</li> <li>•Use PowerShell and Group Policy to manage the Microsoft Enhanced Mitigation Experience Toolkit (EMET), AppLocker whitelisting rules, INF security templates, Windows Firewall rules, IPSec rules, and many other security-related settings.</li> <li>•Install and manage a full Windows Public Key Infrastructure (PKI), including smart cards, certificate auto-enrollment, Online Certificate Status Protocol (OCSP) web responders, and detection of spoofed root Certification Authorities (CAs).</li> <li>•Harden SSL/TLS, RDP, DNS, and SMB against attacks. This includes deploying DNSSEC, DNS sinkholes for malware, SMB encryption, and TLS cipher suite optimization.</li> <li>•Use PowerShell with the WMI service, such as remote command execution, searching event logs, and doing a remote inventory of user applications.</li> </ul>
SEC 542	<p><b>Title:</b> Web App Penetration Testing and Ethical Hacking</p> <p><b>Format:</b> Virtual, online, self-paced training</p> <p><b>Study Time:</b> 60 Hours</p> <p><b>Awarded CPEs/CEUs:</b> 35-40</p> <p><b>Quantity:</b> 3</p> <p><b>Delivery:</b> Within two business days after notification by COR of student identification</p>

Task	Description
	<p><b>Course Contents/Objectives:</b></p> <ul style="list-style-type: none"> <li>•Apply a detailed, four-step methodology to your web application penetration tests: reconnaissance, mapping, discovery, and exploitation.</li> <li>•Analyze the results from automated web testing tools to validate findings, determine their business impact, and eliminate false positives.</li> <li>•Manually discover key web application flaws.</li> <li>•Use Python to create testing and exploitation scripts during a penetration test.</li> <li>•Discover and exploit SQL Injection flaws to determine true risk to the victim organization.</li> <li>•Create configurations and test payloads within other web attacks.</li> <li>•Fuzz potential inputs for injection attacks.</li> <li>•Explain the impact of exploitation of web application flaws.</li> <li>•Analyze traffic between the client and the server application using tools such as the Zed Attack Proxy and Burp Suite to find security issues within the client-side application code.</li> <li>•Manually discover and exploit Cross-Site Request Forgery (CSRF) attacks.</li> <li>•Use the Browser Exploitation Framework (BeEF) to hook victim browsers, attack client software and the network, and evaluate the potential impact that XSS flaws have within an application.</li> <li>•Perform a complete web penetration test during the Capture the Flag exercise to bring techniques and tools together into a comprehensive test.</li> </ul>