



**SECURE  
CONSULTING  
SOLUTIONS**

**CAGE CODE:** 7D7B2  
**DUNS NUMBER:** 074764571  
**TIN:** 472258754  
**NAICS:** 541512, 541519, 541511, 541513, 541690  
**SYSTEM FOR AWARD MANAGEMENT (SAM) REGISTERED**

**Peter Paccione (President)**  
**PPACCIONE@SECURESOLUTIONSDC.COM**  
**(571) 303-9740**  
Certified HUBZone Small Business  
CONUS/OCONUS Support Capability

# CAPABILITY STATEMENT

## COMPANY OVERVIEW

Secure Consulting Solutions, LLC (SCS), a certified HUBZone Small Business, is an Information Technology (IT) Cyber Security services firm with a core focus on Innovative Cyber Security Solutions in Web Application and Mobile Application Security. SCS, founded in 2014 and headquartered in Washington, DC, was established to help commercial and government entities meet the complex and growing technical cyber security challenges faced on a daily basis and strategically plan for the cyber challenges that will be faced in the future.

**SECURE CONSULTING SOLUTIONS, LLC**  
**CERTIFIED HUBZONE SMALL BUSINESS**

**SECURESOLUTIONSDC.COM**

## SERVICES

SCS performs cyber security assessments (both vulnerability assessments and penetration tests) for Information Systems and applications to identify security issues caused by configuration flaws, unvalidated input, non-parameterized queries, lack of system maintenance/patching, misconfigurations and other such issues.

### ■ RED TEAM SERVICES:

Red Team services are designed to provide a safe way for security operations teams to test their ability to effectively defend against cyber-attacks on their compute and development environments. The SCS Red Team specializes in adversary simulation, and by using a variety of tactics, techniques and procedures (TTPs), they have developed expertise to specifically exploit cloud and hybrid environments, as well as DevOps pipelines and processes.

### ■ WEB APPLICATION TESTING:

For many firms, web applications are the most crucial part of their operation. They process credit card orders, allow clients access to their sensitive information, conduct business with partners, and more. It's your job to make sure they continue working, stay secure and present your company's image to the online world. SCS's Web Application Penetration Testing services help to do just that. Our assessment practice specializes in Web Application Penetration Testing and has performed them for companies all over the world. We utilize engineers with advanced certifications, such as SANS GWAPT (GIAC Web Application Penetration Tester), to ensure the most thorough assessments available. From Fortune 100 clients to small businesses, our security consultants work with you to specifically tailor Web Application Assessments to your needs.

### ■ DFARS COMPLIANCE REQUIREMENTS (800-53, 800-171, CMMC):

DFARS compliance refers to meeting the requirements set forth in the Defense Federal Acquisition Regulation Supplement (DFARS), a set of regulations issued by the US Department of Defense (DoD) that governs the acquisition of goods and services by the department. DFARS compliance requires contractors and subcontractors to implement specific cybersecurity controls to protect sensitive information related to DoD contracts, including Controlled Unclassified Information (CUI). The controls are based on the National Institute of Standards and Technology (NIST) Special Publication 800-171, which outlines security requirements for protecting CUI. DFARS compliance is mandatory for contractors and subcontractors doing business with the DoD and failure to comply can result in the loss of contracts and other penalties.

# TRAINING AND CERTIFICATION

SCS is focused on training and development to ensure an effective workforce. SCS is continually adding new capabilities and certifications to increase the depth and breadth of cyber security knowledge and skill that we bring to our clients.

## Cyber Security Certifications and Clearances of SCS Personnel:

- OSCE
- OSCP
- CISSP
- CEH
- Security+
- TS-SCI Clearance

# TOOLS

SCS has expertise and experience in researching, implementing, utilizing, and managing numerous proprietary and open source cyber security tools.

## Partial list of tools in which SCS provides subject matter expertise:

- Tenable Nessus
- HP Fortify Suite
- AppScanner
- Sourcefire
- WebInspect
- Kali Linux
- Cobalt Strike
- Wireshark
- Metasploit
- DbProtect
- Burp Suite
- Kyrptowire
- Nexpose
- Core Impact
- IBM BigFix/Tivoli
- IDA Pro

SECURE CONSULTING SOLUTIONS, LLC  
CERTIFIED HUBZONE SMALL BUSINESS

SECURESOLUTIONSDC.COM

# EXPERIENCED SOLUTIONS



## DEPARTMENT OF STATE

### SECURITY ENGINEERING AND SUPPORT SERVICES

SCS perform mobile device, mobile application, web application, Local Area Network (LAN) and Wireless Local Area Network (WLAN) penetration testing, vetting, and assessments with various tools and techniques (commercial and open source).

Research and test new cyber security tools and techniques. Scan, discover, remediate, securely configure, monitor, and maintain the IT security of all assets on the network. Assess the risk level and threat exposure of the Information System and its assets to cyber threats and vulnerabilities. Present all findings and recommendations to management and senior leadership.



## DEPARTMENT OF HOMELAND SECURITY

### PENETRATION TESTING SERVICES

Conducted onsite penetration tests from an insider/outsider threat perspective. Produced advisory reports to developers, engineers and high level management regarding 0-day exploits, CVE vulnerabilities, and results from manual testing. Identified numerous zero-day vulnerabilities including: RCE, XSS, SQL

Injection and CSRF; rooted FireEye and BlueCoat appliances. Created virtualized lab for exploit creation, malware distribution analysis and security product testing.

Collaborated with external clients to conduct audits and penetration tests and present results to senior management. Performed security reviews of application designs, source code and deployments covering all types of applications (web application, web services, mobile applications, thick client applications, SaaS). Tested over 50 applications ranging from small open source applications to large multi-tier COTs appliances. Developed a virtualized test environment with penetration testing tools including Burp, Kali Linux, WebInspect, AppDectective, Fortify, etc.



**BISHOPFOX**

## BISHOPFOX

### WEB PENETRATION SERVICES FOR GOOGLE PARTNERSHIP PROGRAM

Provided web penetration testing services at Bishop Fox, helped clients such as Kayak.com achieve approval for the Google Partnership Program. This involved conducting a thorough analysis of the website's security vulnerabilities and identifying potential weaknesses that could be exploited by attackers. By leveraging our expertise in web security, we helped ensure that the website met the security requirements necessary to be approved as a Google partner. We work played a crucial role in helping the website achieve its goal and obtain approval for the Google Partnership Program.

Bishop Fox is a cybersecurity consulting firm that specializes in providing comprehensive security services to businesses of all sizes. Founded in 2005, the company offers a wide range of services, including penetration testing, application security, cloud security, network security, social engineering, and more.

For more information, please visit [www.securesolutionsdc.com](http://www.securesolutionsdc.com).