



1. GENERAL INFORMATION

Awarded To: Centurum Information Technology, Incorporated
651 Route 73 North, Suite 107
Marlton, NJ 08053
(800) 376-1226
(856) 751-0286 (fax)
www.centurum.com

DUNS / CAGE Code: 99081143 / 3P825

Award Date: 21 October 2017

Period of Performance: 21 October 2017 – 20 October 2022

Technical Point of Contact: Stephen J. Golle
(843) 266-7502 (direct)
(843) 696-2403 (mobile)
(843) 26607570 (fax)
Steve.golle@centurum.com

Contractual Point of Contact: E. James Iannelli
(703) 415-9384 (direct)
(571) 271-3721 (mobile)
(703) 920-9626 (fax)
Jamie.iannelli@centurum.com

Alternate Contractual Point of Contact: **Lindsay Dugan**
(843) 266-7569 (direct)
(843) 609-5649 (mobile)
(843) 266-7570 (fax)
lindsay.dugan@centurum.com

2. DESCRIPTION OF AVAILABLE SERVICES:

2.a SIN 132-45D (Risk and Vulnerability Assessment (RVA))

Centurum offers Risk and Vulnerability Assessment (RVA) services that include conducting assessments of threats and vulnerabilities; determining deviations from acceptable configurations and enterprise or local policy; assessing the level of risk; and developing and/or recommending appropriate mitigation countermeasures in operational and non-operational situations; specifically:

- Network Mapping - identifying assets on an agreed upon IP address space or network range(s).
- Vulnerability Scanning - comprehensive identification of IT vulnerabilities associated with agency systems that are potentially exploitable by attackers.
- Phishing Assessment - evaluating the level of awareness of the agency workforce with regard to digital form of social engineering that uses authentic looking, but bogus, email requests for information from users or directs them to a fake Website that requests information. Phishing assessments can include scanning, testing, or both and can be conducted as a one-time event or as part of a larger campaign to be conducted over several months.
- Wireless Assessment – performing Wireless Access Point (WAP) detection, penetration testing, or both while onsite at a customer s facility.
- Web Application Assessment – performing scanning, testing, or both of outward facing web applications for defects in Web service implementation that may lead to exploitable vulnerabilities.
- Providing a report on how to implement Web services securely and how to use traditional network security tools and techniques to limit access to the Web Service to only those networks and systems that should have legitimate access.
- Operating System Security Assessment (OSSA) - assessing the configuration of select host operating systems (OS) against standardized configuration baselines.
- Database Assessment - assessing the configuration of selected databases against configuration baselines in order to identify potential misconfigurations and/or database vulnerabilities.
- SIN 132-45A Penetration Testing - conducting and/or supporting authorized Penetration Testing on enterprise network assets.

Applicable NAICS Codes:

Number, Description, and Business Size

541511 Custom Computer Programming Services \$27.5 million

541512 Computer Systems Design Services \$27.5 million

541513 Computer Facilities Management Services \$27.5 million

541519 Other Computer Related Services \$27.5 million

THE REST OF THIS PAGE INTENTIONALLY LEFT BLANK



2.b SIN 132-51 (Information Technology Professional Services)

Centurum offers Information Technology Professional Services that include resources and facilities management, database planning and design, systems analysis and design, network services, programming, conversion and implementation support, network services project management, data/records management, and other services relevant to 29 CFR 541.400.

Centurum's Information Technology Professional Services DO NOT INCLUDE professional services within the scope of SIN 132-45A Penetration Testing, SIN 132-45B Incident Response, SIN 132-45C Cyber Hunt, and SIN 132-45D Risk and Vulnerability Assessment (RVA) Services.

Note: Centurum may employ non-professional labor categories that are incidental to and used solely to support hardware, software, and/or professional services. These non-professional labor categories MAY NOT be purchased separately.

Applicable NAICS Codes

Number, Description, Business Size

- 541511 Custom Computer Programming Services \$27.5 million
- 541512 Computer Systems Design Services \$27.5 million
- 541513 Computer Facilities Management Services \$27.5 million
- 541519 Other Computer Related Services \$27.5 million

3. PROFESSIONAL LABOR CATEGORIES AND FUNCTIONAL DESCRIPTIONS¹

Program Manager – Bachelor of Science and 15 years of directly-related experience. Provides programmatic direction and acts as the principal interface with the Government for all Schedule 70 contract systems and equipment activities.

Project Manager – Bachelor of Science and 10 years of directly-related experience. Directs IT-related projects and ensures achievement of cost, schedule, and technical requirements.

Senior IT Systems Engineer – Bachelor of Science and 10 years of directly-related experience. For Cybersecurity Compliance (CC)- and Information Assurance (IA)-related work, also requires IAT/IAM Level III certification training. Performs IT systems and equipment requirements analysis and assessment; develops specifications and designs; develops logistics solutions; and plans and directs Test and Evaluation activities. Could manage CC and/or IA projects as part of an overarching program.

IT Systems Engineer – Bachelor of Science, to include IAT/IAM certification training, and five (5) years of directly-related experience. Performs IT systems and equipment planning, requirements analysis, design, and test and evaluation. Could contribute during CC/IA activities.

IT Systems Analyst – Bachelor's Degree, to include IAT/IAM certification training, and five (5) years of directly-related experience. Performs IT systems and equipment assessments and analyses in order to make recommendations for improvement.

Senior Cybersecurity Engineer – Bachelor of Science or Master's Degree, to include IAT/IAM certification training and system-/equipment-specific certifications and qualifications, and 10 years of directly-related experience. Leads CC and IA activities to assess risks and vulnerabilities associated with local or enterprise IT environments.

Cybersecurity Engineer – Bachelor of Science, to include IAT/IAM certification training and system-/equipment-specific certifications and qualifications, and eight (8) years of directly-related experience. Performs CC and IA activities to assess risks and vulnerabilities associated with local or enterprise IT environments.

Management Analyst III – Bachelor's Degree and six (6) years of directly-related experience. Supports the IT Program Managers and Project Managers by tracking IT Contract compliance and program/project progress. Collects and collates data, compiles metrics, and prepares reports.

Senior Technical Writer – Bachelor's Degree and eight (8) years of directly-related experience. Leads IT systems and equipment documentation and technical manual development activities.

Subject Matter Expert (SME) III – High School Diploma or GED plus the completion of an advanced level of formal military technical training (equivalent to US Navy "A" and "C" School) or advanced commercial technical training and 10 years of directly-related experience. Relies upon their advanced technical training and experience and management experience to lead or oversee research and studies related to IT systems and equipment operations, maintenance, and training requirements. Identifies IT system training needs and develops IT system training programs and course materials. May deliver IT systems/equipment training.

¹ All Labor Categories EXCEPT Senior Cyber Security Engineer, Cyber Security Engineer, and Management Analyst III are applicable to SINs 132-45D and 132-51. The Senior Cyber Security Engineer and Cyber Security Engineer Labor Categories are applicable only to SIN 132-45D. The Management Analyst III Labor Category is applicable only to SIN 132-51.

Subject Matter Expert (SME) II - High School Diploma or GED plus the completion of an advanced level of formal military technical training (equivalent to US Navy "A" and "C" School) or advanced commercial technical training and eight (8) years of directly-related experience. Relies upon advanced technical training and experience to contribute to IT systems and equipment research and analysis efforts.

Subject Matter Expert (SME) I - High School Diploma or GED plus the completion of formal military technical training (equivalent to US Navy "A" School) or commercial technical training and five (5) years of directly-related experience. Relies upon formal technical training and hands-on experience to provide expert recommendations related to IT systems and equipment operations and maintenance.

Administrative Assistant – High School Diploma or GED and 10 years of directly-related experience. Provides scheduling and meeting support to the IT Contract Program Manager.

Word Processor II – High School Diploma or GED and five (5) years of directly-related experience. Prepares final documents and reports using desktop office applications.

Word Processor I – High School Diploma or GED and one (1) year of experience. Prepares preliminary/draft documents and reports using desktop office applications.