

N00039-18-Q-0003

Attachment 2

SIN	CATEGORY NAME	DESCRIPTION	PWS Section	CLIN
132-8	Purchase of New Equipment	In support of an effort that is within scope of the Task Order	1.15	FFP CLIN 0009, Optional CLINS 1009, 2009, 3009, 4009
132-32	Term Software License	In support of an effort that is within scope of the Task Order	1.15	FFP CLIN 0009, Optional CLINS 1009, 2009, 3009, 4009
132-33	Perpetual Software License	In support of an effort that is within scope of the Task Order	1.15	FFP CLIN 0009, Optional CLINS 1009, 2009, 3009, 4009
132-34	Maintenance of Software as a Service	In support of an effort that is within scope of the Task Order	1.15	FFP CLIN 0009, Optional CLINS 1009, 2009, 3009, 4009
132-40	Cloud Computing Services	The scope of this SIN is limited to cloud capabilities provided entirely as a service such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).	2.1, 2.2, 2.3, and 2.4	Infrastructure as a Service (IaaS) – Reference SIN 132-40 (CLIN 0001, Optional CLINS 1001, 2001, 3001, 4001) Platform as a Service (PaaS) – Reference SIN 132-40 (CLIN 0002, Optional CLINS 1002, 2002, 3002, 4002) Software as a Service (SaaS) - Reference SIN 132-40 (CLIN 0003, Optional CLINS 1003, 2003, 3003, 4003)
132-45A	Penetration Testing	Tasks include but are not limited to: - Conducting and/or supporting authorized penetration testing on enterprise network assets - Analyzing site/enterprise Computer Network Defense policies and configurations and evaluate compliance with regulations and enterprise directives - Assisting with the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems, and processes)	2.6	FFP CLIN 0004, Optional CLINS 1004, 2004, 3004, 4004; T&M CLIN 0005, Optional CLINS 1005, 2005, 3005, 4005; and LH CLIN 0006, Optional CLINS 1006, 2006, 3006, 4006
132-45B	Incident Response	Tasks include but are not limited to: - Collect intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise - Perform command and control functions in response to incidents - Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation	2.6	FFP CLIN 0004, Optional CLINS 1004, 2004, 3004, 4004; T&M CLIN 0005, Optional CLINS 1005, 2005, 3005, 4005; and LH CLIN 0006, Optional CLINS 1006, 2006, 3006, 4006
132-45C	Cyber Hunt	Tasks include but are not limited to: -Collecting intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise - Coordinating with and provide expert technical support to enterprise-wide ComputerNetwork Defense technicians to resolve Computer Network Defense incidents - Correlating incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation	2.6	FFP CLIN 0004, Optional CLINS 1004, 2004, 3004, 4004; T&M CLIN 0005, Optional CLINS 1005, 2005, 3005, 4005; and LH CLIN 0006, Optional CLINS 1006, 2006, 3006, 4006
132-45D	Risk and Vulnerability Assessments (RVA)	Tasks include but are not limited to: • Network Mapping - consists of identifying assets on an agreed upon IP address space or network range(s). • Vulnerability Scanning - comprehensively identifies IT vulnerabilities associated with agency systems that are potentially exploitable by attackers. • Phishing Assessment - includes activities to evaluate the level of awareness of the agency workforce with regard to digital form of social engineering that uses authentic looking, but bogus, emails request information from users or direct 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 - includes wireless access point (WAP) detection, penetration testing or both and is performed while onsite at a customer's facility. • Web Application Assessment - includes scanning, testing or both of outward facing web applications for defects in Web service implementation may lead to exploitable vulnerabilities. Provide report on how to implement Web services securely and that traditional network security tools and techniques are used to limit access to the Web Services.	2.6	FFP CLIN 0004, Optional CLINS 1004, 2004, 3004, 4004; T&M CLIN 0005, Optional CLINS 1005, 2005, 3005, 4005; and LH CLIN 0006, Optional CLINS 1006, 2006, 3006, 4006
132-50	Training Courses	Training for courses normally available to commercial customers, which will permit ordering activity users to make full, efficient use of general purpose commercial IT products.	2.7.10	FFP CLIN 0004, Optional CLINS 1004, 2004, 3004, 4004; T&M CLIN 0005, Optional CLINS 1005, 2005, 3005, 4005; and LH CLIN 0006, Optional CLINS 1006, 2006, 3006, 4006
132-51	Information Technology Professional Services	IT Professional Services over and above initial onboarding and training. Professional services related to the offering such as integration, migration, and other cloud professional services.	2.6	FFP CLIN 0004, Optional CLINS 1004, 2004, 3004, 4004; T&M CLIN 0005, Optional CLINS 1005, 2005, 3005, 4005; and LH CLIN 0006, Optional CLINS 1006, 2006, 3006, 4006