ITES-3S
ITES3-G6CS-ARMY-W81PNH-32

- Customer: Army (USARC)
- Gate: ‘0’
- Step: “0”
- CRM: ITES3-G6CS-ARMY-W81PNH-32
- CIT-Sector: Christopher Stahl

All STAHL USA developed tools, processes, and documents are subject to ©Copyright by STAHL USA and restricted to authorized usage.

Location: Remote Location
Date: 10/14/21

Business Priority Relevance

Client Relationships

Level:	Trusted Vendor	Basis:	Organizational:	Basis: Market

History: Some of the companies in the Stahl channel have experience with this agency and the service branch under ITES-3S. It's STAHL's relationship with this agency that is opening doors to win this opportunity.

Core then Adjacency

Description: In this opportunity, core adjacency will be achieved by identifying a list of vendors who are trusted by this agency. There are some companies in STAHL's channel who have previously worked for this agency, therefore, STAHL is creating a forecast around this buyer for the Clients that have core adjacencies and GAP to the requirements. STAHL is creating a list of vendors who have PP with the Army in Cybersecurity Program Management, Cybersecurity Compliance, Cybersecurity Support, Cybersecurity Daily Operations and Maintenance, and Cybersecurity Continuous Monitoring.

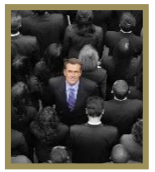
Description: In this opportunity, core adjacency will be achieved by identifying a list of vendors who are trusted by this agency. There

Prime vs. Sub

Intent:	Prime	Basis:	*Strong Past Peformance in functional areas of the PWS*

Dependencies: Prime is a Joint Venture that has the capabilities to fulfill and meet the requirements by GAPPING across all Teaming partners.

Primes Differentiation



Level:	High	Area(s):	Tech/Mgmt	Elements:	Methodology	Staffing

Description: **the** Solution will be developed through the use of Primary Research and a GAP Analysis to the PWS.

Opportunity Overview

Opportunity:	Cybersecurity Support Services			**New/Recompete:**	(R)	**CRM #:**	ITES3-G6CS-ARMY-W81PNH-32
Acquirer:	Army			**Incumbents:**		**Solicitation No #:**	
End User(s):	USARC			**Contract Vehicle:**	ITES-3S	**Contract Type:**	Commercial, Firm-Fixed Priced Contract (Est.)
Location/Place of Performance:	USAR Headquarters Fort Bragg, NC			**Acquisition Type:**	Total Small Business Set-Aside (Est.)		
Prime Interest:				**Acquisition Basis:**			
Prime (P):	T-Four, LLC.	**Sub Value:**	(49%)	**NAICS/PSC:**	541512/ D - IT and Telecommunications	**PWin Change:**	
TOT Value:	$TBD	**(P) Value:**	(51%)	**Opportunity Stat:**	Pre RFP	**RFI/SS:**	October 2021
TOT FTE:		**(P) FTE:**		**Draft RFP:**		**Industry Day:**	
Sector:	Defense	**Channel Team:**	TBD	**Final RFP:**	Dec. 2021 [TBD]	**Prop Due:**	
OPS Exec:	(Thomas Graup)	**ACCT Exec(iPMO):**	Chris	**Orals:**		**BAFO Due:**	
Capture Exec:	(Chris Stahl)	**Prop Lead:**	TBD	**Award Date:**		**Start Date:**	
B&P Estimate:	Unanet T&E	**PrePMO:**	(Richi)	**POP (Period of Performance):**	5 Years (One 12-month base period, starting from notice to proceed with four 12-month option periods)		
Anticipated Personnel Clearance		TS/SCI		**Anticipated Facility Clearance**	TS/SCI		

Brief Program and Scope Description:
The Contractor shall provide non-personal Information Technology (IT) services supporting the United States Army Reserve Cybersecurity. Contractor support will primarily be required in the USAR Head-quarters. The Contractor shall provide cybersecurity support to all USAR organizations for classified and un-classified enclaves hardware, software, data, applications, tools, systems used by the Army. The Contractor shall provide direct support to the USAR with Cybersecurity, Knowledge Management (KM) and Content Man-agement requirements. The Contractor shall provide support in accordance with (IAW) industry best practices as delineated in frameworks such as the Information Technology Infrastructure Library (ITIL). Contractor sup-port is required in all USAR managed enclaves including Non- Secure Internet Protocol Router Network (NIPRNET), Secure Internet Protocol Router Network (SIPRNET).

Background

The United States Army Reserve Command (USARC) has developed and operates the Army Reserve classified and unclassified a centrally managed distributed networks providing consolidated services from Fort Bragg, North Carolina. The unclassified network supports over 72,000 workstations and over 900 servers and 3,000 network devices, supporting approximately 205,000 total Army Reserve personnel to include military, civilian, and contractors. The USAR has over 138 systems and applications currently hosted and utilized on the Army Reserve (NIPR).

Additionally, USARC has over 1200 NIPR sites geographically dispersed throughout the United States and 11 overseas locations. USAR currently has 324 classified Secret Internet Protocol Router (SIPR) locations geographically dispersed throughout our footprint and has coordinated 46 additional SIPR locations utilizing regional Network Enterprise Center (RNEC) services on Camp/Post/Stations (C/P/S).

Scope

The Contractor shall provide non-personal Information Technology (IT) services supporting the United States Army Reserve Cybersecurity. Contractor support will primarily be required in the USAR Head-quarters.

The Contractor shall provide cybersecurity support to all USAR organizations for classified and un-classified enclaves hardware, software, data, applications, tools, systems used by the Army.

The Contractor shall provide direct support to the USAR with Cybersecurity, Knowledge Management (KM) and Content Management requirements.

The Contractor shall provide support in accordance with (IAW) industry best practices as delineated in frameworks such as the Information Technology Infrastructure Library (ITIL). Contractor sup-port is required in all USAR managed enclaves including Non- Secure Internet Protocol Router Network (NIPRNET), Secure Internet Protocol Router Network (SIPRNET).

Objectives

Support the Cybersecurity functional areas to protect and defend USAR information and information systems across NETCOM managed Army DoDIN environments by ensuring the availability, integrity, authentication, confidentiality, and non-repudiation of the system. All Cybersecurity requirements will be per-formed under G6 Information System Security Manager (ISSM) and Contracting Officer Representative (COR) oversight. This also includes restoration of information systems by incorporating identifying, protecting, detecting, responding and recovering capabilities. Draft, maintain, and modify all required documents/plans (Contingency, Incident Response, Change Management, etc.). Support periodic, short or no- notice testing of the plan. Support assess and authorize (A&A) activities of USAR managed systems by conducting research, reviewing documentation and providing input for Risk Management Framework (RMF) packages to the Government for review and approval.

Maintain RMF Executive Packages documentation for completeness and readiness for certification analysis, coordinate with USAR Information Systems Security Manager (ISSM) under G6 Program ISSM (P-ISSM) direction to gather any missing information or resolve other issues precluding certification analysis. Review audit and log files for all systems to ensure that authentication policies are audited and in compliance with the Federal Information Security Management Act (FISMA). Review compliance with current cybersecurity policy, regulations, and directives to ensure secure configuration and operation of all operated and maintained enterprise capabilities and IT assets, recommending corrective actions as required. Provide Cyber-security Capabilities to drive cybersecurity strategy, policy, resourcing and doctrine to optimize and enable de-fense in depth for DoD Information Network operations. It ensures that statutory and regulatory requirements are met, but goes beyond that by pro-actively testing and assessing its networks to identify vulnerabilities and sharpen the skills of cyberspace defenders.

Performance requirements

- Task 1 Program Management
- Task 2 Cybersecurity Compliance
- Task 3 Cybersecurity Support
- Task 4 Cybersecurity Daily Operations and Maintenance
- Task 5 Cybersecurity Continuous Monitoring

Deliverables

STAHL consulting

Table 1

Cybersecurity Operations Branch Deliverables Schedule				
Item	PWS Reference	Deliverable Name	Description	Frequency
1	6.2.3 6.5.1	Security Technical Implementation Guide (STIG) or successor program compliance reporting	Review, verify, and report findings for Security Technical Implementation Guide (STIG) or successor program	As required by COR based on scan result findings Weekly
2	6.3.1	Meetings Minutes	Participation and attendance in ERB, TRB, and CCB	Weekly
3	6.2.3 6.5.1	Device Compliance	STIG or successor programs scans will be conducted via manual and automated	Due every Friday by close of business
4	6.2.3 6.5.1	Device Compliance	Configure devices to meet STIG or successor program compliance	When new STIG policies are developed
5	6.5.3	Threat Assessment	Conduct threat assessment on all USAR managed networks and applications.	Annually
6	6.3.4	Incident Response	Provide support and documentation	Annually
7	6.1.5	Project Plans	Provide project plans for major activities, subject to COB leadership. ie SCA-V, CCRI, IG Inspection	As required

Deliverables

Table 2

Cybersecurity Program Management Branch Deliverables Schedule				
Item	**PWS Reference**	**Deliverable Name**	**Description**	**Frequency**
1	6.1.9.1	SAV Plan	Develop a SAV Plan, including logistics for executing, TTP, develop, schedule, and implement inspection checklist for AIP, define roles/responsibilities of involved parties.	Annual
2	6.1.4 6.1.10	Cybersecurity Training Plan	Develop cybersecurity training plan	Annual
3	6.1.3	Cybersecurity Policy	Prepare and disseminate technical, operational, functional cybersecurity, computer network defense, or cyber defense material to incorporate information presented by vendors, DoD, Army, and Army Reserve	Within 15 business days of request, as required by CPM team
4	6.1.7	RMF Network POA&M report	Prepare and disseminate RMF POA&M report	Weekly
5	6.1.8	Continuous Monitoring Plan	Provide and Develop a continuous monitoring plan	Annually
6	6.1.4	Cybersecurity Task Order Management	Acknowledge, disseminate, track and provide update reporting status	Weekly
7	6.1.6	Report Catalog Maintenance	Provide, develop and maintain document catalog system	Weekly
8	6.1.5	Project Plans	Provide project plans for major activities, subject to CPM leadership. ie SCA-V, CCRI, IG Inspection	As required
9	6.1.5	Audit Support	Provide audit support for hosted applications	As required

Deliverables

Table 3
Performance Requirements Summary

PWS Paragraph	Required Services	Performance Standards	Acceptable Quality Level	Incentives /Disincentives for Meeting or Not Meeting Performance Standards
6.3.2	Draft and update RMF packages and coordinate completion of all RMF activities.	Expiring RMF packages will be completed and submitted to Army CIO/G6 within six months of expiration.	100% of all expiring RMF packages will be completed and submittedto NETCOM CSD within six months ofexpiration.	Positive and negative performance will be documented in monthlyCOR reports.
6.1.3	Draft and update Tenant Security Plans.	Required Tenant Security Plans (TSP)will be reviewed, updated, and completed annually.	100% of TSP's will be reviewed annually and updated or completed asrequired.	Positive and negative performance will be documented in monthlyCOR reports.
6.6	Review and Maintain ATCTS accounts for USAR.	USAR ATCTS accounts will be reviewed for cybersecurity and FISMA complianceand updated as required.	100% of ATCTS accounts will be verifiedor updated to ensure cybersecurity and FISMA compliance at least monthly. New accounts will be updated and verified within 14 business days.	Positive and negative performance will be documented in monthlyCOR reports.
6.5	Maintain and review Audit and log files	Reports are provided by the due date	Reports are provided by the due date 100% of the time	Positive and negative performance will be documented in monthly COR reports.
6.1.7	Maintain and review RMF documentation	Reports are provided by the due date	100% annual review and assessment	Positive and negative performance will be documented in monthly COR reports.
6.1.4 6.1.9.1	Site Assistance Visit Program	Reports are due 3 business days after scheduled SAV is conducted.	80% with a target of 20 sites per year	Positive and negative performance will be documented in monthly COR reports.
6.1.8	Continuous monitoring plan	Due 120 days after contract award and annually thereafter	100% annual review and assessment	Positive and negative performance will be documented in monthly COR reports.