Table of Contents

[Cross Reference Matrix 2-i](#_Toc138722994)

[1.1 Understanding of the Work 2-1](#_Toc138722995)

[1.2 Ability to Implement and Execute the Task/Requirements [PWS 2, 5 and 11] 2-2](#_Toc138722996)

[1.2.1 Validation Support [PWS 5.1] 2-2](#_Toc138722997)

[1.2.2 Training Support [PWS 5.2] 2-3](#_Toc138722998)

[1.2.3 Onsite Support [PWS 5.3] 2-4](#_Toc138722999)

[1.2.4 ISSE Support [PWS 5.4] 2-5](#_Toc138723000)

[1.3 PWS 11.0 Deliverables 2-6](#_Toc138723001)

[2 SUBFACTOR II – STAFFING AND MANAGEMENT APPROACH 2-8](#_Toc138723002)

[2.1 Staffing Approach 2-8](#_Toc138723003)

[2.1.1 Identifying, Recruiting, Preparing, Training, and retention of qualified personnel 2-8](#_Toc138723004)

[2.1.2 Ensuring Appropriate Staffing Mix 2-10](#_Toc138723005)

[2.2 Management Approach 2-11](#_Toc138723006)

[2.2.1 Management for Day-to-Day Operations 2-15](#_Toc138723007)

[2.2.2 Management, Oversight and Control of Resources 2-16](#_Toc138723008)

[2.2.3 Associated Risks 2-16](#_Toc138723009)

List of Abbreviations

| ACRONYM | DEFINITION |
| --- | --- |
| DCSA | Defense Counterintelligence and Security Agency |
| USFFC | United States Fleet Forces Command |
| XYZ | XYZ Inc. |
| C2 | Command and Control |
| RMF | Risk Management Framework |
| A&A | Assessment and Authorization |
| DON | Department of the Navy |
| IT | Information Technology |
| PIT | Platform Information Technology |
| CONUS | Continental United States |
| OCONUS | Outside the Continental United States |
| OPNAV | Office of the Chief of Naval Operations |
| NAVWAR | Naval Information Warfare Systems Command |
| ISSE | Information Systems Security Engineer |
| ISSO | Information Systems Security Officer |
| SCA-L | Security Control Assessor- Liaison |
| SCA | Security Control Assessor |
| SME | Subject Matter Expert |
| NQV | Navy Qualified Validator |
| NMCI | Navy Marine Corps Intranet |
| ONE-NET | Outside the Continental United States Navy Enterprise Network |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Cross Reference Matrix

| Description | SEC. L | SEC. M | PWS Section | Response Section | Page # |
| --- | --- | --- | --- | --- | --- |
| Volume II Technical – Factor II | L.2 | M.1 | N/A | Volume |  |
| Factor II Subfactor I – Performance Approach | L.2 | M.1 | N/A | 1.0 |  |
| PWS 2.0 Scope | L.2 | M.1 | 2.0 | 1.2 |  |
| PWS 5.0 Tasks | L.2 | M.1 | 5.0 | 1.3 |  |
| 5.1 Validation Support | L.2 | M.1 | 5.1 | 1.3.1 |  |
| 5.2 Training Support | L.2 | M.1 | 5.2 | 1.3.2 |  |
| 5.3 Onsite Support | L.2 | M.1 | 5.3 | 1.3.3 |  |
| 5.4 ISSE Support | L.2 | M.1 | 5.4 | 1.3.4 |  |
| PWS 11.0 Deliverables | L.2 | M.1 | 11.0 | 1.4 |  |
| Factor II Subfactor II – Staffing and Management Approach | L.2 | M.1 | N/A | 2.0 |  |
| Staffing Approach | L.2 | M.1 | N/A | 2.1 |  |
| Provide and Retain Staff | L.2 | M.1 | N/A | 2.1.1 |  |
| Ensure Appropriate Staffing Mix | L.2 | M.1 | N/A | 2.1.2 |  |
| Quality of Personnel Resources | L.2 | M.1 | N/A | 2.1.3 |  |
| Management Approach | L.2 | M.1 | 2.2 | 2.2 |  |
| PWS 2.0 Scope | L.2 | M.1 | 2.0 | 2.2.1 |  |
| PWS 5.0 Tasks | L.2 | M.1 | 5.0 | 2.2.2 |  |
| PWS 8.0 Qualifications | L.2 | M.1 | 8.0 | 2.2.3 |  |
| PWS 11.0 Deliverables | L.2 | M.1 | 11.0 | 2.2.4 |  |

1. **FACTOR II – SUBFACTOR I – PERFORMANCE APPROACH**

To assist Commander, US Fleet Forces Command’s [USFFC] cybersecurity initiatives that support training and equipping combat forces, executing command and control (C2) activities, performing operational planning, and executing joint missions, XYZ, Inc. (XYZ) is pleased to respond to USFFC’s solicitation for Navy Risk Management Support. As the incumbent contractor providing these services to USFFC today, XYZ is uniquely positioned to continue our support to the command in its Risk Management Framework (RMF) Assessment and Authorization (A&A) efforts because of our extensive experience across the Department of the Navy’s (DON) major Cybersecurity programs and efforts.

XYZ, Inc. (XYZ), with headquarters located in Arlington, Virginia and offices in San Diego, California; Norfolk, Virginia; Stafford, Virginia; Reston, Virginia; Orlando, Florida; and Charleston, South Carolina, is a management and technology consulting firm specializing in systems engineering, program and project management, process management, cyber security, and Assessment and Authorization (A&A) (formerly Certification and Accreditation (C&A)). XYZ is a Veteran, Woman Owned Business, owned by Ms. Alice Lawaetz and eligible for Small Business Concerns; VOSB - Veteran-Owned Small Business Concerns and WOSB - Women-Owned Small Business Concerns as classified in our SeaPort contract and DUN registration. XYZ currently employs over 160 employees, with annual revenue over the last 3 years averaging approximately $26 million. In support of this solicitation, XYZ has partnered with ABC Security, LLC (ABC) and DEF Consulting LLP (DEF). ABC is a Veteran Owned, Hispanic American Owned, Small Disadvantaged business specializing in Cybersecurity, Engineering and Operations, and Health Information Technology (IT). Notably, ABC has extensive Cybersecurity and RMF experience supporting major Navy commands such as MSC, NAVFAC, and NAVSEA, to include Ashore and Afloat. DEF is (something) with expertise in (stuff, waiting on DEF content), and was chosen as a teammate due to their expertise with RMF tool automation, familiarity with the SCA guidelines and practices due to their current support to the Office of the SCA, as well as their ability to quickly assist with resource surge support if/when required.

XYZ, ABC, and DEF (collectively and individually referred to as the “Team XYZ”) have strategically partnered to bring the following value to USFFC:

***Cybersecurity is a core FWI service, which we have been delivering to the DON for over 20 years***

***Cybersecurity makes up X% of FWI’s delivered services***

***~60% of FWI’s entire Cybersecurity workforce are IAT / IAM III certified***

* ***A proven foundational understanding of the USFFC’s mission.*** We have been successfully supporting the command since September 2012, and the USFFC Navy RMF Validator team since September 2018. Our teams work cohesively between contracts and are fully vested in USFFC’s mission and committed to continued success.
* ***Low transition risk.*** As we are the incumbent providing exceptional service today, we represent minimal transition risk to USFFC at contract award. We have in-place staff ready to work on day one, continuing their exceptional support.
* ***A wealth of Cybersecurity expertise.*** We have a core competency of talented individuals that meet Cybersecurity Workforce requirements and can understand and navigate the RMF process across all system types successfully (e.g., cloud, enterprise, network, site, application, system, Platform IT (PIT)). They can expertly support various types of authorizations including Ashore, Afloat, Continental United States/Outside the Continental United States (CONUS/OCONUS), and Type authorizations.
* ***Deeply engrained in all major Navy RMF programs efforts.*** Besides our USFFC work, we are also embedded in key organizations like the Office of the Navy Authorizing Official (NAO), the Office of the Security Control Assessor (SCA), Office of the Chief of Naval Operations (OPNAV), and Naval Information Warfare Systems Command (NAVWAR). We have superior internal reach back capabilities within our teams to help us understand the changing RMF landscape and solve operational challenges.
* ***Full-service RMF operation.*** Not only do we perform all RMF steps and several RMF roles (e.g., Navy Qualified Validator (NQV), Information Systems Security Engineer (ISSE), Information Systems Security Officer (ISSO), NAO Analyst, PSO Analyst, Security Control Assessor- Liaison (SCA-L)), but we also provide proven and innovative training, tools, and processes that aid in expediting the RMF process.
* ***Agility.*** We are agile, and have repeatedly proven that we can easily adapt to emerging/shifting mission needs.

## Understanding of the Work

In addition to our current support to USFFC, our cybersecurity Subject Matter Experts (SMEs) and NQVs have supported A&A processes for critical enterprise programs and systems such as Navy Marine Corps Intranet (NMCI), OCINUS Navy Enterprise Network (ONE-NET), MyNavyHR, LOG IT, LI2S-MC, Navy ERP, and E2S. Team XYZ performs in all critical roles throughout the RMF process, including NQV, ISSO, ISSE, NQV, as well as NAO, PSO, and SCA Analysts. Not only do we provide RMF support to commands, but we also support the Office of the NAO, Office of the SCA, and OPNAV. Our range of support across the RMF steps, roles, and processes enables Team XYZ to serve as a full-service RMF shop, providing proven and innovative training, tools, and process development that aids in expediting the RMF activities.

## Ability to Implement and Execute the Task/Requirements [PWS 2, 5 and 11]

Our qualifications, breadth, and depth of knowledge across the Navy’s vast network environment and success rate is proven. Notably, we’ve reviewed 221 A&A packages specifically for USFFC. Our cyber professionals provide USFFC stellar support through all RMF steps under the USN RMF Process Guide (RPG) and the Navy SCA RMF Risk Assessment Guide.

### Validation Support [PWS 5.1]

Beginning with system categorization (Step 1), we will assist the program in populating the USN RMF Security Categorization Form, based on the National Institute of Standards and Technology (NIST) SP 800-60, ensuring Classification, Applicable Overlays, Releasability and National Security System (NSS) determination was applied correctly. We will also ensure all information types are present based on “what the system is and what the system does.” We will consult with the PSO to confirm applicability and proper signing authority. Continuing to Step 2, we will assist Program representatives in applying the baseline control set based on system confidentiality, integrity, and availability. We will also ensure the overlays are added and tailored as appropriate. Finalizing Step 2, we assist the Program in populating all Enterprise Mission Assurance Support Service (eMASS) fields required to produce an accurate System Security Plan. After the Program completes testing (Step 3), we will validate the Body of Evidence (BOE), and the SCA Office signs the Security Assessment Report (SAR) (Step 4); the package enters Step 5. If necessary, we will assist Program representatives in drafting and proofing High-Risk Escalation documentation if a high-risk determination is made. During validation, our team will review the organization’s test results for technical and non-technical control and related Assessment Procedures (AP) to determine implementation compliance. An in-depth analysis of Information System (IS) artifacts will be performed to support a thorough validation and risk assessment. We will analyze categorization, control selection and implementation, and the security plan to develop the Security Assessment Plan (SAP) to properly test and evaluate all assets and software (SW) within the site’s accreditation boundary. Onsite, we will gain a thorough understanding of the IS, perform testing, interview program team members, and observe the work environment to assess compliance with program policies, Standard Operating Procedures (SOPs), and physical and environmental controls. The team will perform the required testing by conducting both remote and onsite validation activities of the IS for all RMF controls and APs, including technical testing (Assured Compliance Assessment Solution (ACAS) vulnerability scans, Security Technical Implementation Guide (STIG)s), NIST SP 800-53A controls, Ports, Protocols, and Service Management (PPSM), architecture drawings, and all other related artifacts provided by the Program, local, Navy, and federal policy compliance to support the Navy SCA risk assessment. We will review all completed testing and document all findings in accordance with policy guidance, including false-positive and misleading results. We will upload all required artifacts to eMASS, mark security controls appropriately, and document findings properly in the Plan of Action & Milestones (POA&M). We will scrutinize the testing results against all applicable controls, trace APs and findings to the POA&M, and evaluate all results for the SCA to be captured in the SAR. Accuracy of Residual Risk for each is validated to support the SAR, reflecting compliance status of all Security Controls and overall risk level of the IS. We will provide executive summaries for the SCA Liaison that accurately describe the IS risk level, to facilitate SCA signature. We will also brief site leadership and personnel regarding requirements and finding results. Ultimately, the SCA will submit the SAR to the NAO which is used to support their authorization decision. (5.1.1; 5.1.2)

Once an Authorization to Operate (ATO) is granted, we will help address any ATO stipulations and provide support in monitoring the security controls (Step 6). We will provide guidance in determining the proper controls to assess during an Annual Security Review (ASR), based on the