

**Securities and Exchange Commission**

**Program Management Office (PMO) Support Services**

**Solicitation Number: SECHQ1-15-R-0004**

**Technical**

This proposal shall not be duplicated, used, or disclosed – in whole or in part – for any purposes other than to evaluate this proposal. If however, a contract is awarded to Technik, Inc., as a result of – or in connection with – the submission of this data, the Government shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the Government’s right to use information contained in this proposal if it is obtained from another source without restriction. The data subject to this restriction is contained on sheets marked with the legend. “Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this proposal.”

**Technik, Inc., agrees to all terms, conditions, and provisions included in this solicitation**



*This proposal or document includes sensitive information that FSIS shall not disclose outside the Agency and its service providers that support management activities and administrative functions. To gain access to this sensitive information, a service provider’s contract must contain the clause entitled "Access to Sensitive Information". Consistent with this clause, the service provider shall not duplicate, use, or disclose the information in whole or in part for any purpose other than to perform the services specified in its contract. This restriction does not limit the Government's right to use this information if it is obtained from another source without restriction. The information subject to this restriction is contained in all pages in this proposal response.*

**Submitted by:**

**Technik, Inc.**

CMMI Maturity Level 3 Certified   
(Dev&Svc V1.3)

ISO 9001:2008 Registered

12950 Worldgate Drive, Suite 230

Herndon, Virginia 20170

([www.technikinc.com](http://www.technikinc.com) )

703.981.6991

Date Submitted: August 20, 2014

DUNS Number: 168319569

Cage Code: 33XT9

Business Size: 8(a) Small Disadvantaged Business

**Submitted to:**

**US Department of Agriculture**

Food Safety & Inspection Service (FSIS)

Attn: Joseph Pishioneri

1400 Independence Ave., SW

Room 3165 South

Washington, DC 20250

**Volume I: Technical Quotation**

**Public Health Information System (PHIS) Design and Development**

Solicitation #AG-3A94-S-15-0070

US Department of Agriculture (USDA) Food Safety & Inspection Service (FSIS)

# Abstract / Table of Contents (2 pages, outside of 30 pages)

A two-page summary should be provided abstracting the quotation contents in language understandable to a layperson. The abstract shall indicate full acceptance of the solicitation requirements or specify any exception.

## Technik Abstract

Technik, Inc., (“Technik”) a CMMI Maturity Level 3 certified, ISO 9001:2008 registered small 8(a) company is pleased to submit our proposal in response to Solicitation # AG-3A94-S-15-0070 to provide design and development support services to US Department of Agriculture (USDA) Food Safety & Inspection Service (FSIS).

Technik has collaborated with USDA since 2008 and currently maintains APHIS IT Web-based systems that support certification, accreditation, registration, permitting, and other licensing activities. The systems we support provide tactical support of mission critical work for USDA by integrating with the U.S. Department of Treasury www.pay.gov site to process fee payments. They support USDA data exchange with systems used by other Federal Government agencies such as Customs and Border Protection (CBP) that are also involved in the inspection and movement of commodities under APHIS' regulatory authority. Technik has transformed the individual knowledge afforded by these engagements into corporate knowledge by institutionalizing best practices and lessons learned from USDA engagements. Our teams understand USDA’s mission.

Technik strives to constantly seek the right balance of breadth, depth, and manageability and has carefully chosen to team for this opportunity to provide support services to USDA FS. As part of our overall strategy for providing quality client delivery teams, we selected a partner who has a steadfast commitment to high quality HR IT client service provided with integrity, quality, flexibility, and creativity, which aligns with our corporate philosophy.

Sustained quality excellence is one of our core beliefs and provides the basis of our client delivery experience. Our quality control plan implements best practices from ISO 9001:2008. The operations and maintenance approach described in our proposal are rightly aligned to the CMMI-SVC Maturity Level 3 recommendations. Technik’s proposed application development process supports an iterative planning and feedback loop enabling development teams adapt to changing business requirements and deliver software that meets desired business needs.

***Quotation Abstract***

Technical Approach – BPA Setup

BPA Technical Work Plan

Corporate Experience

Management Plan

Personnel, Qualifications, and Staffing (including Resumes)–

Performance Work Statement

**Technik, Inc. acknowledges and accepts all solicitation requirements, including terms and conditions, representation and certifications, and technical requirements as outlined in the solicitation, and we do not take exception to any of the information contained therein.**

## Table of Contents

[1. Abstract / Table of Contents (2 pages, outside of 30 pages) 1](#_Toc427917116)

[1.1 Technik Abstract 1](#_Toc427917117)

[1.2 Table of Contents 3](#_Toc427917118)

[2. Factor A - Technical Approach – BPA Setup 6](#_Toc427917119)

[2.1 Understanding of the BPA 6](#_Toc427917120)

[2.2 Understanding of Mission and Objectives of FSIS and PHIS 6](#_Toc427917121)

[2.3 Staffing Plan 6](#_Toc427917122)

[2.3.1 Staffing Critical Issues and Risk Identification and Mitigation 7](#_Toc427917123)

[2.4 Subcontractor Responsibilities and Rationale 8](#_Toc427917124)

[2.5 CMMI Certification 8](#_Toc427917125)

[3. Factor B - Technical Work Plan – BPA task order 9](#_Toc427917126)

[3.1 PWS Strategies, Operations and Procedures 9](#_Toc427917127)

[3.1.1 Application Development and Support (PWS 1) 9](#_Toc427917128)

[3.1.2 Support Services (PWS 2) 10](#_Toc427917129)

[3.1.3 Transition to Support (PWS 3) 10](#_Toc427917130)

[3.1.4 Task Order Management (PWS 4) 10](#_Toc427917131)

[3.2 Project Plan 10](#_Toc427917132)

[4. Factor C - Corporate Experience 11](#_Toc427917133)

[5. Past Performance 14](#_Toc427917134)

[6. Factor E - Management Plan 15](#_Toc427917135)

[6.1 Administrative Structures / Organizational Resources 15](#_Toc427917136)

[6.2 Operating Procedures 15](#_Toc427917137)

[6.3 Managing the Workforce 16](#_Toc427917138)

[6.4 Quality Control 16](#_Toc427917139)

[6.4.1 Quality Performance Standards 17](#_Toc427917140)

[6.5 Cost Containment 18](#_Toc427917141)

[7. Factor F - Personnel, Qualifications, and Staffing 19](#_Toc427917142)

[7.1 Key Personnel 19](#_Toc427917143)

[7.2 Staffing Plan 20](#_Toc427917144)

[7.2.1 Organization and Lines of Authority / Responsibility 20](#_Toc427917145)

[7.2.2 Staff Continuity and Ability to Back-Fill 21](#_Toc427917146)

[8. Appendix 1: Resumes 23](#_Toc427917147)

[8.1 Project Manager, Satish Venkatesan 23](#_Toc427917148)

[8.2 Senior Business Analyst, Kristina New 25](#_Toc427917149)

[8.3 Deputy Project Manager/Agile Coach, Blair Aubertien 26](#_Toc427917150)

[8.4 Quality Assurance Lead, Meganoosh Avakian 31](#_Toc427917151)

[8.5 Software Engineering Manager/Solutions Architect, Vijay Thottikkattu 32](#_Toc427917152)

[8.6 Lead Developer, Bhaskar Nalluri 34](#_Toc427917153)

[8.7 Letter of Commitment, Technik Employees 37](#_Toc427917154)

[8.8 Letter of Commitment, Meganoosh Avakian 38](#_Toc427917155)

[9. Appendix 2: Performance Work Statement 40](#_Toc427917156)

[9.1 Introduction Section 40](#_Toc427917157)

[9.2 Background Section 40](#_Toc427917158)

[9.3 Scope of Work Section 41](#_Toc427917159)

[9.4 Tasks Section 42](#_Toc427917160)

[9.5 Delivery Schedule Section 54](#_Toc427917161)

[9.6 Performance Standards Section 56](#_Toc427917162)

[9.7 Assumptions Section 56](#_Toc427917163)

[9.8 Constraints Section 56](#_Toc427917164)

[9.9 Government Furnished Equipment Section 56](#_Toc427917165)

[9.10 Government Furnished Information Section 57](#_Toc427917166)

[9.11 Place of Performance Section 57](#_Toc427917167)

[10. Appendix 3: Compliance Matrix 58](#_Toc427917168)

[11. Appendix 4: CMMI Level 3 Certification 61](#_Toc427917169)

[11.1 Technik CMMI Recognition of Achievement 61](#_Toc427917170)

[11.2 Technik CMMI Appraisal Disclosure Statement 62](#_Toc427917171)

[12. Appendix 5: Information Technology Systems Security Information 70](#_Toc427917172)

[12.1 Security Laws and Regulations 70](#_Toc427917173)

[12.1.1 Federal Information Security Management Act 70](#_Toc427917174)

[12.1.2 Office of Management and Budget Circular A-130 70](#_Toc427917175)

[12.2 Security Standards and Best Practices 71](#_Toc427917176)

[12.2.1 National Institute of Standards and Technology 71](#_Toc427917177)

[12.2.2 International Organization for Standardization 71](#_Toc427917178)

[12.2.3 SANS (SysAdmin, Audit, Network, Security) 72](#_Toc427917179)

[12.2.4 Center for Internet Security 72](#_Toc427917180)

[12.2.5 ORGANIZATION’S SUPPORTING PROGRAMS 72](#_Toc427917181)

[12.3 Technik Security Policies 72](#_Toc427917182)

[12.3.1 Physical Security 73](#_Toc427917183)

[12.3.2 Personnel Security 73](#_Toc427917184)

[12.3.3 System and Data Identification 74](#_Toc427917185)

[12.3.4 Incident Response Program 75](#_Toc427917186)

[12.3.5 System Security Plan 75](#_Toc427917187)

[12.3.6 System Development Life Cycle 76](#_Toc427917188)

[12.3.7 Configuration Management 76](#_Toc427917189)

[12.3.8 Training and Awareness Program 77](#_Toc427917190)

[12.3.9 System Documentation 78](#_Toc427917191)

[12.3.10 Disaster Recovery 78](#_Toc427917192)

[12.4 CERTIFICATION AND ACCREDITATION (C&A) PROGRAM 79](#_Toc427917193)

[12.4.1 Certification Process 79](#_Toc427917194)

[12.4.2 Accreditation Process 82](#_Toc427917195)

[12.4.3 Post Accreditation Activities 82](#_Toc427917196)

[12.5 SUMMARY 83](#_Toc427917197)

[13. Appendix 6: Signed Rules of Behavior Document 84](#_Toc427917198)

[14. Appendix 7: Section 508 Product Assessment Template 86](#_Toc427917199)

**List of Figures**

**List of Tables**

**No table of figures entries found.**

# Factor A - Technical Approach – BPA Setup

## Understanding of the BPA

Technik understands that the Public Health Information System (PHIS) Design and Development contract will provide new and expanded functionality to PHIS applications for the Food Safety & Inspection Service (FSIS). This includes software that is currently in production as well as future software that will be deployed during the contract period. In providing this support, it is expected that best practices and standards such as CMMI will be fully embraced in performing a broad range of required services.

Technik will be responsible for understanding and adhering to USDA-specific SDLC processes and procedures. Compliance with these processes will be audited by the Quality Manager and corrective actions will be identified and implemented. All team members are expected to correct the actions identified in audits and work product reviews to ensure the highest quality possible for all work products and deliverables. In supporting this contract, some critical contract objectives include:

* Transition-In and efficiently assume responsibility with no loss of service, minimal disruption and/or negative impact on the USDA staff and user community.
* Efficiently and effectively develop solutions that meet or exceed the needs of PHIS users and that adhere to a proven standard development methodology.
* Establish and adhere to efficient and effective project management processes.
* Provide guidance, engineering, and strategic thinking to assist USDA in augmenting its strategic plans.

In summary, we understand that the services performed under this contract involve systems that are critical to USDA’s mission, and as such, our plan involves a combination of well-defined and executed processes, a robust set of enabling technologies, and a cadre of skilled and experience personnel that are available immediately upon contract award.

## Understanding of Mission and Objectives of FSIS and PHIS

## Staffing Plan

Technik is fully committed to providing USDA PHIS with highly qualified personnel that meet or exceed the position requirements. We provide a cohesive team of proven leaders and managers who have worked together on previous assignments similar to the PHIS contract, each offering compelling skills and experience to successfully fulfill the requirements outlined in the solicitation.

Our staffing plan for USDA PHIS will consist of a BPA Management Team to oversee all the projects and tasks. Consisting of the Program/Project Manager, Deputy PM/Scrum/Release Manager and Solutions Architect, the BPA Management Team will provide senior leadership and guidance to the rest of our staff on all aspects of PHIS work. In addition, Technik will also staff Technical Team Leads (TL) for each task area (Export, Import, Domestic and Predicative Analytics). Each TL brings software development expertise and strong leadership capabilities to the team. In addition to the TLs, each task area will be staffed with experienced developers, analysts, testers and technical writers utilizing the labor categories below. For more information regarding staffing please reference, section *7.2 Staffing Plan.*

|  |  |  |
| --- | --- | --- |
| **Title and Responsibilities** | **Labor Category** | **Services Needed** |
| Program / Project Manager | Program Manager I |  |
| Software Engineering Manager / Solutions Architect | Project Lead – Application Systems and Programming III |  |
| Senior Business Analyst | Computer Systems Analyst III |  |
| Database Administrator | Database Administrator I |  |
| Domestic Inspection Team - Software Team Lead | Internet/Intranet Application Specialist I |  |
| Import Activities Team - Software Team Lead | Internet/Intranet Application Specialist I |  |
| Export Activities Team - Software Team Lead | Internet/Intranet Application Specialist I |  |
| Predicative Analytics Team - Software Team Lead | Internet/Intranet Application Specialist I |  |
| Senior Programmer | Application Developer II |  |
| Intermediate Level Programmer | Software Engineer II |  |
| Business Analyst | Computer Systems Analyst II |  |
| Technical Writer | Technical Writer II |  |
| Tester | Test Engineer II |  |
| Deputy PM/ Scrum/Release Manager | Project Lead – Application Systems and Programming III |  |
| Configuration Manager | Software Support Engineer III |  |
| Information Assurance Security Officer (IASO) | Data Security Analyst III |  |
| Senior QA Analyst | Computer Systems Analyst III |  |

### Staffing Critical Issues and Risk Identification and Mitigation

Technik has identified the risk areas, which have the potential to compromise either our initial staffing, or our ability to maintain a responsive work force once on contract. The table below presents those critical issues and risk areas and discusses our mitigation approach.

|  |  |  |
| --- | --- | --- |
| **Risk Area** | **Concern / Issue** | **Risk Mitigation Strategy** |
| Skill Mix | Failure to understand client’s requirements results in an improper skill mix | * Analyze existing task, interview client’s and incumbent employees * Maintain position descriptions which are responsive to present and future client requirements * Review position descriptions with Key Personnel who understanding client requirements * Constantly review skill mix on contract to ensure ongoing adequacy of staff |
| Selected staff is over- or under- qualified | * See mitigation identified above * Attempt to identify work which is suitable and transfer employee * Attempt to identify work elsewhere in the company and transfer employee * Make skill mix adjustment in the best interest of client |
| Incorrect quantities of skills proposed | * See mitigation identified in both blocks above * Analyze schedule and hour allocations on existing tasks |
| Recruitment | Critical Labor Categories are hard to attract | * Educate individuals on Technik benefits during interviews * Maintain list of qualified internal candidates and applicants * Leverage personnel cutbacks in other parts of industry * Consider technical agencies |
| Work Fluctuations | Short term work surges caused by unanticipated or critical tasks require specialized skills | * Maintain communications in areas where surges may occur * Maintain a list of qualified candidates who will accept temporary assignments * Consider technical agencies |
| Cutbacks which require disposition of valuable resources | * Find temporary labor coverage within company * Provide services to assist with job placement, leaving individual with a positive image and potential for recall |
| Subcontracting | Subcontracting may compromise performance, schedule, and cost | * Subcontract only when absolutely necessary * Dedicate sufficient management attention to ensure low risk performance |

## Subcontractor Responsibilities and Rationale

There are no subcontractors proposed on the PHIS Design and Development contract.

## CMMI Certification

Technik, Inc. has been appraised at Maturity Level 3 on the Capability Maturity Model Integration (CMMI) for Development and Services, v1.3, based on a Standard CMMI Based Appraisal Method for Process Improvement (SCAMPI) Class A, v1.3 Appraisal, completed on September 25, 2012. The *CMMI Recognition of Achievement Certificate* and *Appraisal Disclosure Statement* are provided in Appendix 4.

# Factor B - Technical Work Plan – BPA task order

Section L: In the Technical Work Plan, quoter’s shall fully detail and explain the strategies, operations and procedures that they propose to fulfill the tasks outlined in their proposed PWS (PWS instructions included below in “Additional Quotation Instructions”. The quoter should organize, by task, the descriptions of work to be performed and the methods to be used. Each task should be presented under a separate heading with the same numerical designations as presented in the proposed PWS and mapped to the objectives outlined in the Statement Of Objectives (SOO) (attachment #2). The Technical Work Plan should present detailed information on how the quoter plans to accomplish the tasks proposed in the quoter’s proposed PWS. Included in the Technical Work Plan should be a project plan, outlining and detailing the projected dates and deliverables to be provided in accomplishing the task.

Section M - The Government will evaluate the adequacy of the quoter’s Technical Work Plan:

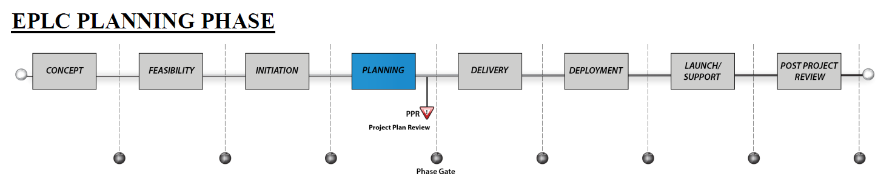
The quoter demonstrates a thorough understanding of the goals of the PHIS requirements as evidenced by the creativity and thoroughness shown in the planned execution of projects associated with the projects objectives.

Evidence of specific methods and timelines for completing each discrete task associated with fulfilling the goals of the PHIS design and development is clearly shown and supported in the quoter’s project plan. The quoter demonstrates a thoughtful and unique approach for developing and executing the design and development techniques required to achieve or enhance the objectives of task order 1.

## PWS Strategies, Operations and Procedures

Quoter’s shall fully detail and explain the strategies, operations and procedures that they propose to fulfill the tasks outlined in their proposed PWS (PWS instructions included below in “Additional Quotation Instructions”. The quoter should organize, by task, the descriptions of work to be performed and the methods to be used. Each task should be presented under a separate heading with the same numerical designations as presented in the proposed PWS and mapped to the objectives outlined in the Statement of Objectives (SOO) (attachment #2). The Technical Work Plan should present detailed information on how the quoter plans to accomplish the tasks proposed in the quoter’s proposed PWS.





### Non-Phase Specific Activities (PWS 1)

#### Ramp up Knowledge Transfer – Transition IN (PWS 3)

The Technik Knowledge transfer plan is structured to assume full contract responsibility upon completion of the 45 day Phase-In period and incorporates HR, property management, and knowledge transfer activities required to successfully phase-in incumbent personnel, GFE, and current systems without interrupting services.

**Knowledge Transfer Manager**

Technik appoints our Program Manager, Mr. Satish Venkatesan, as the Knowledge transfer manager to oversee transfer of knowledge. As Transition Manager, Mr. Venkatesan (USDA develops and submits a Knowledge Transfer Plan (KTP) that documents transition activities to assume complete responsibility for successful PHIS operations. The KTP provides coverage for activities essential to Technik’s ability to perform an on-schedule, responsive, and efficient transition process including the following.

* Appoint a Transition Team for this contract to seamlessly assume on-going work.
* Implement proven processes and industry best practices culled from established contract transition processes and Technik lessons learned archive to achieve a smooth transfer of responsibilities while simultaneously having little or no impact on PHIS operations during the transition period.

The KTP also serves to strengthen operational readiness to assume full contract responsibilities and transition tasks on Day One of the contract by focusing on several areas of significance to PHIS operations both during and subsequent to the transition. These areas include:

**Maximum retention of the incumbent staff members:** The plan aims for incumbent retention, thus capturing crucial incumbent skills and experience, and addresses all other aspects of the transition to assure a non-disruptive and on-schedule completion.

**Understanding the mission and processes essential to the PHIS support:** Our Transition Team leadership includes key Team Technik management positions, senior project managers, and Team Technik executive management, each with relevant backgrounds in similar fields and detailed understanding of GITISS support mission and operations.

**Control and management of problems, issues, and risk:** This plan includes the identification and mitigation of possible problems, issues, or risks having the potential to jeopardize transition processes, schedule, and ultimate success. For each anticipated obstacle, corrective responses are in place and able to control, manage, and reverse any negative impact resulting from such obstacles. Thus, this Phase-In Plan incorporates mitigation plans to minimize any problems, issues, or risks emerging during the transition period.

Our Phase-In approach has several key components that allow us to assume on-going work, which are shown below and mapped to the proposal section where they are discussed.

**Administering the Knowledge Transfer Plan (KTP)**

Immediately upon award, Technik conducts a PHIS Kick-Off to meet with the CO, COTR and other USDA stakeholders to confirm the KTP, identify the Government personnel with whom we must immediately meet. The emphasis is on transferring knowledge of “as-is” operations from the incumbent staff and Government stakeholders to Team Technik. We meet with USDA senior management to phase-in PHIS -specific technical knowledge from the current contractor to Team Technik. After reading and analyzing the Standard Operating Procedures (SOPs), project plans, and pertinent technical documentation, we conduct information-gathering sessions with USDA and the incumbent staff to observe current operations. Throughout the phase-in period, we update USDA with daily activities regarding processes, accomplishments, and risks. Key activities include:

**Kick-Off Meeting** - Meet with the designated USDA COTR, CO and other FSIS stakeholders to identify key issues pertinent to both phase-in and ongoing operations. We confirm our Knowledge transfer Plan and identify other Government personnel stakeholders.

**Meet with Other PHIS Personnel** - Schedule meetings with other key Government personnel to familiarize them with our phase-in activities, understand the technical challenges they face, and identify any near-term critical activities that are in process.

**Meet with Incumbent Management** – Schedule meetings with the incumbent Program Manager, HR, and Security Officer to initiate transfer of personnel data, open projects and tasks, technical procedures, GFP, and security PIV data lists to facilitate badge transfers.

**PHIS Workforce Online Portal**– Upon contract award, Team Technik launches the Team Technik GITISS Workforce online portal. This site provides a detailed schedule of phase-in events, including our Open House times and locations. It features company information, job descriptions, ability to submit resumes, applications, benefit and contact information.

**Identification and Capture of Critical Personnel** - All critical positions at this stage are identified and offer letters and HR paperwork are signed. All security transfer and PIV card activities are initiated, ensuring critical personnel are ready to phase-in to Team Technik on day 1 of the contract year.

**Identification and Capture of Non-Critical Personnel** - Non-critical personnel are ready to assume full responsibility from the incumbent contractor on day 1 of the contract year. To achieve this, offer letters and HR paperwork are signed and personnel clearance processing and activities are initiated rapidly so that any issues are resolved prior to day 1 of the contract.

**Knowledge Transfer** – Team Technik eliminates single-point failures by implementing a proactive Knowledge Retention Plan and transferring individual knowledge to corporate knowledge. Our Phase-In Team works closely with the COTR and CO to understand and plan a smooth phase-in of ongoing work and take necessary actions to support new requirements in a timely manner. Information is collected for ongoing work including the status/progress of the tasks, current assignee(s), next steps to complete, and timeframe for phase-in.

**Knowledge Retention** – The purpose of the Technik Team’s knowledge transfer process is to develop a broad and in-depth understanding and knowledge of our client’s business, applications, technology, and staff while protecting the GSFC’s business assets. We employ a variety of techniques, including assessments, workshops, peer reviews, and SOPs, to obtain information from the retained incumbent staff.

**Operational Readiness Review (ORR)** – The ORR ensures that Team Technik is ready to assume all GITISS contract functions. This review consists of both Team Technik and GITISS stakeholders.improvements so that performance can be measured.

**Security Verification Processing**

Technik works with the USDA Security Division and the incumbent contractor after award to take immediate steps to begin the process to transfer security clearances, entry badges, and computer privileges for incumbent personnel so there is no disruption of services. Our Security Officer (SO), Mary Battaglia has over 25 years of industry security experience. She handles any needed transfers of security clearances and all paperwork related to security forms and compliant fingerprint cards for their respective employees. Ms. Battaglia was instrumental in the incumbent capture security transfer activities at KSC for the ITSS contract. She ensured that all security and badging concerns were handled expeditiously. Our SO provides regular updates on the team’s security onboarding status and works with the USDA stakeholders and with the USDA Security Division to ensure compliance with all USDA directives and remove any obstacles to the process.

**Knowledge Transfer Communications**

Our phase-in process establishes a communications program throughout the ninety (90) day transition phase for identifying, communicating and mitigating risks. As appropriate, contingency plans are instituted to minimize disruption of service. Our plan begins with joint agreement on a schedule for critical events that take place between announcement and cutover. The interaction continues with daily updates and weekly status review meetings with USDA stakeholders and outgoing contractor.

**Close Coordination and Communication with outgoing contractor and Government Personnel** –Technik executes a communications program that stresses maintaining current service delivery and transparency with USDA stakeholders. Our Phase-In Team closely coordinates issues and status daily, both among the team and with USDA through an online dashboard, daily reporting and regularly scheduled meetings. Communication activities include the development of communication paths with USDA to gain insight into the status of the current workload. We have weekly Phase-In Readiness Reviews (status meetings) with GSFC Stakeholders in addition to daily status updates.

|  |  |  |
| --- | --- | --- |
| **Interface POC** | | **Coordination Tasks** |
| **USDA** | USDA CO | * Participate in weekly tagups to discuss phase-in progress/milestones * Identify and initiate tasking * Review/approve plans and other deliverables * Develop and review Service Level Agreements and Performance Metrics |
| USDA COTR | * Participate in weekly tagups, if desired * Provide data and information regarding MAPI goals and objectives; changes in scope; other SOW-related items |
| USDA IT Resources | * Access and coordinate computer applications, assets, and resources and licenses * Coordinate IT Security requirements and IT Security Plan approval * Transfer computer access requests |
| Security/Badging and Control Office | * Finalize badging requirements and interfaces for PIV clearance |
| Property Management | * Participate in inventories, establish property custodian POCs |
| **Predecessor Contractors** | Incumbent Representative | * Identify tasking/staffing and discuss support areas and overlaps in ongoing work * Identify/discuss risk areas and processes * Support property inventory and Safety and Health baseline survey * Transfer property * Acquire employee records (Names, seniority dates, job title) |

Team Technik will transfer this contract from the incumbent contractor, in a professional and cooperative manner. We believe that we should approach this time as a learning process for both incoming and outgoing contractors. Our first priority during phase-in is to establish interfaces with the COTR and predecessor contractor management with the goal of minimizing disruption to ongoing work and fostering professional long-term relationships with key participants and GSFC organizations. To accomplish our plan, primary interfaces with Predecessor Contracts and NASA individuals and coordination of task are identified in the Table 7.1. Our strategy is to work with the predecessor contractor to identify the support needed to successfully transition work and personnel, ensuring a seamless transition to GSFC. The Team Technik Phase-In Team will work with the incumbent contractor regarding transition of ongoing operations, transfer of GFE, transfer or novation of licenses and agreements, and with handling problem and issues during transition. Additionally, we will request access to incumbent personnel for knowledge transfer, job shadowing, and recruiting activities.

**Communication with Personnel** – Keeping personnel up to date on the status of their work, benefits and their role in the project is an essential element of successful phase-in. A coordinated effort of complete and transparent communication between all levels of Team Technik and existing personnel is a fundamental step in the phase-in process. We use a variety of approaches to communicate with the GITISS workforce, including Open Houses, a phase-in web portal and other relevant methods. Key messages focus on retention and phase-in activities.

**Phase-In Schedule**

The overall responsibilities of the Transition Team include among others:

• Identifying, establishing, and maintaining customer contractual and organizational interfaces.

• Re-badging incumbent personnel and badging new personnel.

• Addressing IT security issues and tasks.

• Initialization of Team Technik’s NASA-proven Task Management System (EPICS)

**Phase-In Risk**

Risks are inherent in contract phase-in; however, we follow a solid Risk Management approach. Common phase-in risks are already known and our experienced Phase-In Team is well equipped to establish mitigation strategies. We provide status of identified risks and mitigation strategies at daily meetings and at the weekly Transitional Readiness status Meetings. A sampling of initial risks and mitigation strategies is noted in the Table below

| **Table V2-A7-4. Potential Transition Risk & Risk Response. The response will mitigate, accept, research, and monitor expected outcome and resulting risk level.** | |
| --- | --- |
| **Potential Risk** | **Risk Response** |
| **Loss of Incumbent Staff.** If a significant percentage of incumbent staff leave before, at, or shortly after the transition, there will be reduced effectiveness, efficiency, an increased likelihood we will not be able to maintain continuity of operations. The risk of data loss will increase. | MITIGATE. Team Technik will use the same proven, effective procedures on many prior contracts, with the expected result of capturing over 90% of the incumbents while actually improving their morale. We will give bonuses for accepting employment within one week of offer. Our 401(k) provides immediate vesting – and a competitive compensation and benefits package. We will work with employees to instill confidence in Team Technik’s commitment to communicate openly and honestly with all employees and treat them fairly and equitably. As a further mitigation, to reduce the consequences in the event of employee departures, we will have a Hot Queue of prequalified candidates (including Team Technik’s reachback) to backfill openings. The result of this mitigation plan will be reduction of the risk to a very low level. We are also paying special bonuses to those with critical skills (if necessary). |
| **Incumbent Contractor Cooperation:** If the incumbent staff/contractor proved to be uncooperative, it would impact such things as transfers of software licenses, hardware maintenance agreements, and government property. | MITIGATE. We will advocate weekly status meetings between the incumbent staff/contractors and Team Technik for oversight. We will also document all meetings through minutes and action item tracking. We have found most staff/contractors to handle this situation professionally. However, mitigation is not entirely under our control, so this will be considered a significant risk. |
| **Knowledge Transfer:** If we do not quickly achieve currency of knowledge of all activities and issues, failsafe transfer of responsibilities from the incumbent to Team Technik cannot be seamless. | MITIGATE. Team Technik proposes participation during transition by our management staff in GSFC meetings associated with activities performed by the incumbent staff. We also propose shadowing of incumbent staff during the conduct of their responsibilities on a non-interfering basis. Also, a Team Technik member firms are experienced with GSFC’s varied infrastructure. Consequently, if our proposals are acceptable, we see this as becoming a very low risk. |
| **Senior Staff Retirements:** If a significant percentage of staff eligible to retire does so, there may be a loss of expertise, with inability to perform specific activities, greatly increasing risk of loss of data, failure to support GSFC customers, increasing likelihood we will not be able to maintain continuity of operations. | MITIGATE. We will undertake multiple actions to mitigate this risk. First, we have *analyzed* positions held by senior staff and determined that backups with some experience are actually available in each case. However, we will put our primary emphasis on preventing them with a series of measures. We will assure employees they can collect retirement from their prior company and earn salary as part of Team Technik. We will also use signing bonuses, retention bonuses, 401(k) immediate vesting; credit for prior years of service, and a competitive compensation and benefits package. Team Technik may offer special bonuses to Senior Staff for inducing them to stay. We will work with employees to instill confidence in commitment to Team Technik. We will communicate openly and honestly with all employees and treat them fairly and equitably. As a further mitigation step for reducing the consequences in the event of employee departures, we will have a Hot Queue of pre-qualified candidates (including Technik reachback) to backfill openings. The result of this mitigation will be reduction of the risk to a very low level. |
| **Incumbent Contractor Retaining Employees:** If mission-critical employees who have significant seniority with the incumbent contractor choose to stay with the contractor, or if the incumbent contractor actively seeks to entice these employees to stay but to work on other contracts, we would experience a loss of staff and experience potentially impacting quality and capability of ensuring mission continuity. | For these and other employees, we will also use signing bonuses, retention bonuses, 401(k) immediate vesting; credit for prior years of service, and a competitive compensation and benefits package. We will work with employees to instill confidence in commitment by Team Technik to communicate openly and honestly with all employees and treat them fairly and equitably. As a further mitigation step for reducing the consequences in the event of employee departures, we will have a Hot Queue of prequalified candidates (including Technik reachback) to backfill openings. The result of this mitigation plan will be risk reduction to a very low level, based on our experience with many successful transitions over the years. |
| **Customer Interface:** If we do not establish and maintain a positive customer interface from day one, there is a significant likelihood that the customer will find it difficult to gain confidence in our team. There will be additional workload and stress on GSFC staff, with reluctance to discuss process improvement after peak activity period. | MITIGATE. Team Technik will use dedicated Transition Teams with specific actions and milestones to establish positive customer interfaces, as described in detail in our transition plan. Our past experience with using dedicated transition teams on transitions strongly indicates that selecting Team Technik effectively mitigates this risk to a very low level. |
| Full staff to be provided by the Technik Team– incumbent staff not transferred | * + Use our Knowledge Transfer process to glean knowledge from the incumbent.   + Draw from our employee base to staff the GSFC program.   Team Technik has a continuous pipeline of GITISS specific pre-screened candidates to ensure any back-fill positions are staffed quickly and efficiently |
| Issues arise in the technical environment that would prevent smooth phase-in of project management services to the Technik Team | * + Hold a series of status sessions with GSFC and a readiness assessment to verify Day-1 readiness to accept management responsibility.   + Work through GSFC to provide a fallback contingency with the incumbent as appropriate so that service levels are maintained.   + Present a draft baseline project plan to GSFC for review at the kick-off meeting. |
| **ITAR Restrictions:** | MITIGATE: We will hire U.S. Citizens only for this contract until the restriction is lifted or the government works out something whereby International collaboration is possible |

**Transition Quality Management**

To ensure a seamless Phase-In, Team Technik sets measureable expectations and ensure that accountability is established for gathering, analyzing and reporting the phase-in metrics. Our Quality Management Plan provides an understanding of GSFC requirements and expectations for quality and performance, an understanding of existing GITISS processes and best practices that are used on the contract, an approach to train all employees and subcontractors on the GITISS processes, and establishment of measures and other feedback mechanisms for improvement.

#### Transition to Support [Transition Out]

At the conclusion of our contract, Technik supports transition to FSIS PMO the duties, activities, and functions of tasks and tools for the PHIS contract. Technik PM will meet with the transition PMs from each contractor to ensure that all concerns and issues have been met and addressed appropriately. Once the customer’s transition PM has formally accepted the transition. Transition out support include:

* Maintains existing staff on-site throughout the transition period.
* Immediately prior to the transition, stand up a transition team to facilitate the activities necessary for successful
* Conduct weekly Knowledge Transfer training sessions at the outgoing/in coming vendor locations and government sites to
* Review FootPrints Tickets, SCRs and RFCs;
* Review TFS requirements for PHIS
* Describe program office requirements that have not yet been implemented
* Provide estimates of the resources needed to complete all unfinished work
* Describe system operations including schedule of operations;
* Review and describe eCert and CBP requirements and configurations
* Detailed summary as well as work papers and files for work that is in progress.
* Explanation of ongoing issues, how they are being dealt with, options and long-range plans
* Update to all requirements, design documents and plans
* Any current security issues raised by the contractor or for which the contractor has supported fact finding; and
* The known status of any ongoing reviews by outside parties including CIO, independent C&A reviewer, IV&V reviewer, OIG, or GAO
* Throughout the transition continue work in accordance with the approved project schedule and work breakdown structure (WBS) in place.
* As part of this transition, turn over all documentation, information and knowledge to the Government,
* For this transition, knowledge transfer will take place via various methods. Technik PM will coordinate formal classroom training sessions to be conducted by Technik. These sessions will focus on the specific IT concerns related to the database tasks and activities. The incumbent PM will also coordinate formal classroom sessions to be conducted by the Technik Configuration Manager. These sessions will cover documentation requirements and organizational processes and assets.
* Meet with the FSIS bi-weekly (twice a month) to discuss the progress and status of the knowledge transfer.
* Utilize an updated MS Project Schedule during this meetings, as well as discuss any risks or concerns.
* the established transition checklist in order to determine Task Order Management (PWS 4)

### EPLC Process of Planning (PWS 2)

### SDLC Requirements Analysis Phase (PWS 3)

### SDLC Design Phase (PWS 4)

### SDLC Development Phase (PWS 5)

### SDLC Integration /Acceptance Phase (PWS 6)

## Project Plan

Included in the Technical Work Plan should be a project plan, outlining and detailing the projected dates and deliverables to be provided in accomplishing the task.

Evidence of specific methods and timelines for completing each discrete task associated with fulfilling the goals of the PHIS design and development is clearly shown and supported in the quoter’s project plan. The quoter demonstrates a thoughtful and unique approach for developing and executing the design and development techniques required to achieve or enhance the objectives of task order 1.

# Factor C - Corporate Experience

|  |  |  |  |
| --- | --- | --- | --- |
| Veterinary Services (VS) - Digital Signature Pilot | | | |
| Agency | United States Department of Agriculture (USDA), Animal and Plant Health Inspection Service (APHIS), Veterinary Services (VS) | | |
| Contract # | AG-32KW-D-13-0288 | | |
| Contract Value | $609,290.84 (confirm) | Contract Type | Firm Fixed Price |
| Duration of Task | 9/30/2013 - 9/29/2014 | DUNS | 168319569 |
| Point of Contact | Patrick J McFall, 970-494-7214, [patrick.j.mcfall@aphis.usda.gov](mailto:patrick.j.mcfall@aphis.usda.gov) | | |
| Type of Services Provided | | | |
| As a prime contractor, Technik provided USDA APHIS VS with application development support. The primary objective of this contract was to develop a digital signature workflow as VS documents are presented for signing, review, and acceptance. Technik integrated the VSPS application with a 3rd party esignature enterprise and upgraded the VSPS importation forms to accept digital signatures. In order to ensure integrity of the process, Technik implemented digital signature technology in the Veterinary Services Processes Streamlining (VSPS) online as well as off-line applications.  Our SME, along with developer and PM, worked with USDA engineers and management staff to identify technical solution requirements for the Digital Signature project. Technik conducted requirements development and prototype testing, documenting the results for applicability to the USDA environment. All requirements and analysis were subject to Technik quality and peer reviews to ensure compliance with USDA and NITC guidelines, policies, and procedures.  Digital Signature was subject to Independent Testing and Verification (IT&V) to ensure that the software was robust, stable, and secure. We used a three-phased approach: the Discovery phase was conducted in collaboration with USDA and included reviews, information gathering, and planning activities needed to scope and target test activities. The Establishing a Foundation phase established the required test requirements, including the number and types of tests. The Implementation and Execution phase was when Technik designed, developed and executed the test cases, in collaboration with VS staff. We recorded test results, documented and reported defects (in daily testing meetings), and tracked all defects in ClearQuest, until their resolution.  Technik developed a complete release package that included technical documentation, security assessment reports, and deployment scripts. We collaborated with NITC to prepare the appropriate production environment and assisted with the implementation of new infrastructure /server requirements.  Technik developed and implemented a controlled, responsive, and adaptive framework for Continual Service Improvement on the Digital Signature project. We identified improvements to current practices through continuous monitoring while maintaining strict compliance to applicable Federal, USDA and NITC standards. | | | |
| Problems Encountered and Corrective Actions | | | |
| There were no problems encountered with the USDA Digital Signature Pilot contract. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| USDA APHIS VS Software Development and Support | | | |
| Agency | United States Department of Agriculture (USDA), Animal and Plant Health Inspection Service (APHIS), Veterinary Services (VS) | | |
| Contract # | AG-32KW-D-110599, AG-32KW-D-08-0378, AG-32KW-08-0122, AG-32KW-D-09-0448, AG-32KW-S-09-0318, AG-32KW-D-08-0106 | | |
| Contract Value | $2,304,020.50 (confirm) | Contract Type | Firm Fixed Price |
| Duration of Task | 3/24/2008 – 12/14/2012 | DUNS | 557258436 |
| Point of Contact | Tom Dalton, DV United, 703-623-2702, [thomas.dalton@tdginc.com](mailto:thomas.dalton@tdginc.com) | | |
| Type of Services Provided | | | |
| Technik, as a lead member of a Service Disabled Veteran Owned Small Business Enterprise joint venture company (DV United), provided software development, requirements analysis/design, project management, and operations and maintenance services to the Federal Government, including the USDA APHIS VS. Technik provided all labor and management for these Task Orders. All phases of the USDA APHIS Program required Technik to respond to System Change Requests (SCRs) from managers, users, and customers regarding defect repairs and software modernization. Stakeholders deposited SCRs continually monitored by Technik. Technik also responded to an aggregate of SCRs accumulated over a period of several months. Technik was required to enhance, repair, update and address security issues; produce cost, benefits and needs analyses documents; develop, test, and implement approved upgrades for various user communities using an intermingled but disparate array of servers and platforms.  This program was performed under six task orders as explained below.   * *Task Order 1 - VS Software Development and Support* - The VS Software Development and Support task order required Technik to provide DME and O&M services to the Veterinary Services Process Streamlining (VSPS) system. * *Task Order 2 - VSPS Import and Export Product* - the VSPS Import and Export TO required Technik to integrate the functionality of Veterinary Services Permits Issuance Tracking System (PITS) with VSPS by creating new functionality within VSPS for the Facilities/ Establishments for the Import of Animal Products (A/E) and the VSPS Facilities module. Successful completion of these tasks enabled VS to retire the PITS application. * *Task Order 3 - IBM Websphere Portal Direction* - Technik supported the USDA eGovernment initiative to provide web access and to deploy web applications through a web portal framework using the IBM Websphere Portal. As a part of the Task order, Technik developed J2EE applications, portlets, web services, and utilities needed to interface with the Websphere Application Server and Websphere Portal environment. * *Task Order 4 – NAIS Allocator Enhancements –* DME activities for this task included developing an improved user interface for the ALLOCATOR application; develop application level secure webservices to support data interchanges and remove inconsistencies in code while adhering to a more standard National Animal Identification System (NAIS) development model. * *Task Order 5 – NAIS Performance and Scalability Analysis -* The purpose of this Statement of Work (SOW) is to contract for testing and analyzing the performance and scalability of the NAIS to prepare for the program’s anticipated future performance needs. * *Task Order 6 - National ID Reporting Function Enhancements Requirements* – This order tasked Technik to gather and document requirements related to improving the NAIS reporting function.   **Support the VSPS, NAIS and APHIS Portal Teams in Architecture, Analysis, Design, Development, Maintenance and Reporting.** Technik gathered the requirements to develop the detailed analysis and expand the capabilities within the VSPS, NAIS and APHIS Portal systems to meet all of the product deliverable requirements. We performed discovery of requirements for the modification of VSPS Import and Export enhancements, NAIS allocator enhancements, APHIS Portal content and NAIS Reporting Functions Enhancements. We modified the VSPS and NAIS database structure and data content as necessary to support the development. We provided assistance and training to the Veterinary Services and NAIS staff on the use and maintenance of the modified VSPS Import and Export and NAIS Allocator systems. We updated all existing system documentation to reflect the modified applications including the system architecture report. We performed routine maintenance on the SQL Server Databases.  **VSPS Import and Export, NAIS Allocator and APHIS Portal Program Maintenance Support and Accessibility.**During the contract period of performance, modifications originating from users and management were required to be made to existing versions of the VSPS Import and Export application, NAIS Allocator and the APHIS Portal application. Upon modification approval by the COTR or PM; development, testing, evaluation, implementation and maintenance was performed in accordance with applicable USDA VS regulations. Technik performed changes and modifications to existing VSPS Import and Export, NAIS Allocator and Portal Server program code as required in the form of system change requests submitted by USDA VA liaisons. We examined the contents of the SCR to determine the work efforts required, and then worked with the USDA liaisons to rearrange work schedules and priorities as required to meet the demands. We analyzed costs, processed and tested modifications to the VSPS Import and Export, NAIS Allocator and Portal Server, in the form of SCRs, to keep the system current with requirements.  **Release Management and System Documentation.**As a part of our release management process, we provided release management plans and deployment plans for every scheduled release. Source code was provided to the program manager upon successful completion of system integration and testing. We developed System Standard Operating Procedures (SOP), to include software test plans, software test procedures, software test descriptions, maintenance, trouble resolution and escalation procedures, and disaster recovery plans. We developed a repository containing system designs and definitions within Technik Solutions Framework. We developed and provided user and system administrator training manuals. We delivered deployment plans and product release specifications document at the end of each release. | | | |
| Problems Encountered and Corrective Actions | | | |
| There were no problems encountered with the USDA Software Development and Support contract. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SEC, IT Support Services | | | |
| Agency | Securities and Exchange Commission (SEC) | | |
| Contract # | SECHQ1-08-F-8122, SECHQ1-11-F-0189, SECHQ113C0065 | | |
| Contract Value | $6,598,608.72 | Contract Type | Firm Fixed Price |
| Duration of Task | 10/2008 – 6/2017 | DUNS | 168319569 |
| Point of Contact | Janak Rajani, SEC, 202-551-3722, rajanij@SEC.GOV | | |
| Type of Services Provided | | | |
| As a prime Contractor, Technik currently provides onsite IT Support Services within the SEC, Division of Corporation Finance (CorpFin) under a multiple year, $6.5mil contract. Our staff provides CorpFin with technical and functional staff to support software development, enhancement, maintenance, and support services for all production applications, databases, SharePoint sites, other internal websites and Business Objects reports. The scope also includes support of Software Development Life Cycle (SDLC) processes; software configuration; quality assurance; system integration; system administration; software testing; research into new technologies; develop reports, metrics and dashboards.  Our approach to SEC development tasks follows an Agile / Scrum methodology. By using an iterative process, we are able to adapt to the SEC’s needs in a flexible way while still maintaining a disciplined release management process. At the end of each development cycle (i.e. “Sprint”), we demonstrate the new functionality to gather feedback. Rather than waiting until the end of the project, this gives the SEC the opportunity to change direction and/or reprioritize the Product Backlog prior to the start of the next Sprint.  As part of our development support, all enhancement and modification efforts begin with a comprehensive review of artifacts for all systems applications. This includes a review of architecture diagrams, system design documents, and technical specifications of system components. Technik analysts provide CorpFin with requirements that cover aspects of functionality, usability, reliability, performance, suitability and security. We understand that each requirement should be definitive, measurable, testable, and defined to a detail level which that allows for comprehensive system development and deployment. We follow a 7-step requirements elicitation process which includes project definition, research, discovery, analysis, validation and final documentation.  Detailed test plans, test results, test scripts, and test cases are developed for all development tasks. Our team has dedicated testing resources who work with developers to build documentation and perform unit tests, functional tests, capacity and load tests, survivability tests, and Section 508 compliance tests. All test plans and scripts comply with the Requirements Traceability Matrix and are be delivered to the COR for review and approval.  Technik staff coordinate with CorpFin and upon concurrence, move releases from development to production environments - performing all code, database, configuration, and data transformation tasks as needed for each release. Before deployment of an application, a complete implementation packet is submitted to the COR for review, which contains all the required documents for the SEC’s Office of Information Technology (OIT) deployment process.  Technik continually examines, documents and implements current operational processes, such as for configuration management, release management, change management, risk management, source control procedures, applicable SEC briefings, user administration, user support, and development standards. When gaps are identified, our staff resolve the deficiencies, corrects the documentation and implement the updates processes. Technologies used include: SQL, .NET, C#. | | | |
| Problems Encountered and Corrective Actions | | | |
| There were no problems encountered with the SEC Corpfin IT Support Services contract. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| NASA, Information Technology Support Services (ITSS) | | | |
| Agency | National Aeronautics and Space Administration (NASA) | | |
| Contract # | NNK13OM02Z | | |
| Contract Value | $19,900,000.00 | Contract Type | Firm Fixed Price |
| Duration of Task | 2/28/2013 – 9/30/2015 | DUNS | 168319569 |
| Point of Contact | Gloria McIntosh, 321-867-1270, [gloria.a.mcintosh@nasa.gov](mailto:gloria.a.mcintosh@nasa.gov) | | |
| Type of Services Provided | | | |
| Technik provides support for the IT Directorate at NASA Kennedy Space Center (KSC). Technik staff supports the Information Technology and Communications Services (IT) Directorate in the overall management and direction of design, engineering, development, integration, and operations of information technology and communications systems and services for KSC institutional and NASA program customers.  Technik provides expertise, leadership, and guidance in the design, development, and sustaining engineering for the entire life cycle (Concept Studies to Decommissioning) of new and existing applications, process and supporting data center services. Our analysis and design support also includes the review of operational system designs and equipment specifications. These reviews are from a technical standpoint with particular emphasis on system engineering, installation, operation and maintenance. Our project team reviews unique engineering design equipment specifications with emphasis on new system implementation issues.  Technik provides NASA KSC expertise in software development management and formulation for the application and integration of advanced health management software tools, methods and capabilities for command and control of KSC ground support equipment and systems. Our staff formalizes engineering processes to document high-level user requirements, conducting all formal technical reviews such as SCR, SRR, PDR, CDR, TRR and ORR, review of project documentation, and tailoring of NASA Governance NPRs. The Technik project team establishes sound, compliant Configuration Management (CM) practices and processes and ensures the test planning, test conduct and problem reporting activities are thorough prior to turnover to operations. Our team works closely with the technical community to help create and maintain high level technical architectures. | | | |
| Problems Encountered and Corrective Actions | | | |
| There were no problems encountered with the NASA ITSS contract. | | | |

# Past Performance

Technik is confident in our ability to deliver services in a timely manner. We are proud of our past performance and resulting customer satisfaction. The following table details the point of contact that the Corporate Experience questionnaire was submitted to.

|  |  |
| --- | --- |
| **Contract Name** | **Contact information for Questionnaire Submission** |
| USDA, Digital Signature Pilot | Patrick J McFall, 970-494-7214, [patrick.j.mcfall@aphis.usda.gov](mailto:patrick.j.mcfall@aphis.usda.gov) |
| USDA Software Development and Support | Tom Dalton, DV United, 703-623-2702, [thomas.dalton@tdginc.com](mailto:thomas.dalton@tdginc.com) |
| SEC, IT Support Services | Janak Rajani, SEC, 202-551-3722, rajanij@SEC.GOV |

In lieu of a questionnaire, please reference the CPARS system for the NASA ITSS contract. Technik’s DUNS number is 168319569.

# Factor E - Management Plan

Technik brings high quality support, and our innovative management approach provides consistent planning, execution, and control. Technik offers USDA the right set of skills to succeed with the mission goals and objectives, and meet the challenges of the future. Our management team is in place, known, and respected within USDA and Federal Government user community.

## Administrative Structures / Organizational Resources

Technik has established BPA level organization structure, seen on page xx, figure xx, that consists of a Technik Corporate Support Team, a BPA Management Team and TechnicalTeam Leadership. This structure enables an extremely cost-effective application of technical and programmatic personnel for USDA.

* **Corporate Support Team** functions include: Human Resources maintains a continual focus on career development, benefits administration, employee relations, performance management, and development of a positive corporate culture that is supportive of the employee’s growth and success. Talent Acquisition proactively and continually develop a pipeline of qualified candidates. This effort is led by Technik recruiters and coordinated with each of our team members. Accounting and Finance support all administrative financial aspects of this program. This includes time accounting, invoicing, and employee payroll. Contracts Management support the PHIS program by maintaining contractual relationships, tracking key dates and obligations, and oversight of funding levels.
* **BPA Management Team** is comprised of our Program Manager, Deputy Program Manager and Solutions Architect who play instrumental roles in overseeing all BPA projects.
* **Technical Team Leadership** - Technik Task Leads (TL) are responsible for the technical performance planning activities of our management approach for individual Task Orders (TO). Each TL directs and controls the technical performance of the TO through supervisory meetings with task personnel and the identification of specific activities for each. They will monitor accomplishments and daily activities, and confer with subordinates on a daily basis to address status and issues.

## Operating Procedures

Quoters shall present a Management Plan showing the strategies for implementing their proposed technical work plan through administrative structures and operating procedures to successfully carry out each task.

Technik brings an established and successful history of innovative and strategic IT consulting expertise for clients. We understand our role as prime vendor—especially on a Blanket Purchase Agreement (BPA) —and pledge to bring depth of experience to achieve strategic IT solutions, and consistent design and development support. Most important, and one of our most distinct differentiators is the fact that we bring a culture of learning, partnership, communication, and innovation. We continuously help our clients improve with the evolution of technology. Furthermore, our proven practices using strategic analysis, governing frameworks, and IT roadmaps are predictors of future success on USDA tasks. We are confident in the use of these practices and that it ensures consistent and efficient management, positive and regular communications with all stakeholder personnel, and quickly resolves cross-organizational issues. Technik’s best-of-breed management methodology follows four simple steps:

**Plan:** We tailor our management structure to meet USDA needs. We selected xxxx. Mr. Venkatesan is responsible for the management and performance of all TOs. This focused corporate attention/oversight assures USDA of our commitment to attentive management and successful technical performance.

**Perform:** Technik provides open and complete transparent communication during delivery. We allow ready access to project plans and schedule, regular progress reports, and work deliverables. We manage ongoing technical direction through regular daily formal and informal meetings with USDA. Monitoring, tracking, and reporting activities include performance management, quantitative risk management, and quality assurance.

**Measure:** We follow a continuous improvement process on all projects as part of our standard procedures. At the heart of this is ongoing measurement of project performance. A Quality Assurance and Quality Control Plan will be developed specifically for the needs of USDA and includes detailed performance metrics. Using this open approach, Technik and USDA will be able to detect variances and issues early and mutually agree upon any corrective action plans necessary.

**Improve:** Technik draws on lessons learned and focused improvement plans based on metric results collected and feedback from customers. We conduct regular project and program reviews with our staff to implement positive adjustments to our work processes and deliverables.

To provide a secure, auditable trail from award to completion and facilitate collaboration, Technik implements a USDA Virtual Performance Center (VPC), a secure central repository of project information that allows USDA stakeholders to access all Technik tools, metrics, schedules, reviews, templates, training, and deliverables. The VPC provides performance transparency using real-time reporting to simplify surveillance, monitor performance, and seek opportunities for continuous improvement of all tasks.

## Managing the Workforce

Quoters shall explain how they propose to manage and coordinate operations and personnel working for the contractor, including any subcontractors and consultants, as well as the quoter’s employees.

## Quality Control

Our commitment to providing exemplary quality through strong and effective procedural controls in our services and support is based firmly on our accredited Quality Management System (QMS), which defines standards by which we measure the effectiveness of the services we provide to our customers. As an ISO 9001:2008-registered and CMMI Maturity Level 3 appraised organization, Technik applies standard, repeatable processes to ensure that our procedures are defined, repeatable processes are followed, and that we meet and exceed our clients’ required performance standards.

Our approach for managing systems and software project quality for this contract is driven from the quality management philosophy of independence and robust peer-review assessments in each phase of the Software Development Life Cycle (SDLC). This provides greater improvement of quality and management of risk. The QA Officer will work with the internal project team and with stakeholders to establish a clear and common understanding of project requirements.

Throughout the SDLC, we implement quality control by using rigorous process and product audits, reviews, and activity monitoring. Results provide indicators to aid in managing the system development process. Key components include:

* **Monitoring** -Activities are reviewed on a routine basis to verify implementation of the quality system and to assess performance adequacy, including achievement of established performance metrics.
* **Audits -** Project processes and products are evaluated against the documented processes, procedures, and requirement standards. The QA Officer selects the types of methods and activities needed to objectively evaluate both process and product quality based on lifecycle, client drivers, configuration items, and deliverable products. The QA Officer provides independent reviews of selected processes, activities, and documentation throughout projects lifecycle.
* **Reviews -** The project QA Officer participates in, observes, or conducts reviews as appropriate in accordance with the review work product process defined for the project. In addition, the QA Officer will conduct independent reviews of the project process adherence and product standards. An example would be to have an independent observer witness the testing process.

Our staff understand that quality indicators provide real-time and actionable information to teams. This is a proactive approach to quality and allows for continuous improvement. As a result staff can drive products and process improvements in real time. Management techniques and processes are detailed in the Technik Quality Assurance and Quality Control Plan, which is submitted within 20 days of contract kick-off.

### Quality Performance Standards

| Performance Requirements | Performance Indicator | Performance Standard | Performance Surveillance Method |
| --- | --- | --- | --- |
| On-time submission of Deliverables | Contractor shall submit all deliverables to USDA on or before due date/time. | Meets scheduled date | Receipt of each deliverable by date/stamp postmark of electronic delivery. |
| Requirements verification against delivered product | Comparison of requirements features as documented and validated in the detailed RTM | 100% of the requirements are met | USDA test team will validate deliverable against the requirements. |
| Critical software defects | Number of critical defects per release cycle | No critical defect shall be detected after software has been transferred from the contractor development environment to the test environment. | Manual and automated testing by USDA tester. After remedy of critical defect retesting will occur by USDA testers |
| Software defects | Number of critical defects per release cycle | <6 defects shall be detected after software has been in operation for 1 month | Reports from production users where analysis has determined that a true defect is present |
| Overall customer satisfaction | Customers are satisfied with the contractor’s teamwork and performance | 80 percent of the customers are satisfied with the contractor’s teamwork and performance | Survey distributed to customers by USDA PM |
| Overall User satisfaction | Users are satisfied with the software application | 80 percent of users express that they are satisfied (or greater than satisfied) | Survey distributed to users by USDA PM |

## Cost Containment

Project costs will be controlled at two levels, the total contract level and the individual task order level. Since each task bears its pro-rated share of the total overhead, the sum of all task costs equals the total contract cost. Our proposed approach to effective project cost control includes: controlling contract cost items within prescribed limits; controlling task order costs to remain within the planned cost estimates; using our on line project management tools to proactively monitor incurred versus planned costs at both contract and task order levels; identifying and reporting task order and total contract costs which vary from their planned values; and implementing corrective actions to bring incurred costs in line with planned costs.

* **Contract Level Cost Control** - Costs at the contract level are the sum of all costs borne by each task order issued under the contract. Technik will monitor these costs weekly, monthly, quarterly, and annually. Contract cost elements will be compared with the actual incurred cost elements and a project performance report will be generated to enable our PM to monitor our cost performance against our cost control commitments. When total incurred contract costs are projected to exceed planned contract costs, the PM will initiate a Red Flag Report to the COR, which will detail the overage and the mitigation strategy to prevent it.
* **Task Level Cost Control** - Effective control of task order costs depends mainly on the accuracy of the initial planning and estimating process. Using our project planning tools, skill levels, labor hours, and numbers of FTEs will be allocated to each task order activity. Once an approved schedule has been developed and labor categories and hours assigned for each task order, the required costs for travel, subcontract support, and equipment or materials are also identified for each task order activity. The resource requirements, schedule milestones, deliverables, and total task order costs are then documented and presented in weekly status meetings and monthly progress reports.
* **Earned Value Management** – Technik strives to adhere to strict EVM cost and schedule controls. Our EVM reports provide valuable insight into the progress of tasks and projects. Our EVM solutions conforms to all the 32 guidelines stipulated in ANSI Standard EIA-748, Industry Guidelines for Earned Value Management Systems. We design and deliver Earned Value Management Systems (EVMS) reports including designing WBS, setting up Baseline Budget Control accounts, and work measurement by control accounts and follow PMI PMBOK guidelines.

# Factor F - Personnel, Qualifications, and Staffing

Technik is fully committed to providing USDA with highly qualified personnel that meet or exceed the position requirements. We provide a cohesive team of proven leaders and managers who have worked together on previous assignments similar to USDA PHIS.

## Key Personnel

The following table details the key personnel and their qualification to perform on the USDA Design and Development effort. All proposed staff have submitted Letters of Commitment and are available immediately upon award. All key personnel resumes are provided in *Appendix 1, Resumes.*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Name, Title** | **Labor Category** | **Proposed Staff Qualifications** | | | | | | |
| *Satish Venkatesan,* Program/ Project Manager | **Program Manager I** | Intro  Intro  Intro  Intro | | | | | | |
| **LOE Hours** | Non Proj Spec - 280 | Phase 1  504 | Phase 2  112 | Phase 3  44.8 | Phase 4  112 | Phase 5  67.2 |
| *Blake Aubertien* Deputy PM/Scrum/ Release Manager | Project Lead – Application Systems and Programming III | Ms. Aubertien holds a Bachelors of Science in Integrated Science and Technology. She brings over 15 years of specialized experience as a highly talented project manager, Agile coach and SME. Her other qualifications include knowledge of Scrum processes, Rally (Agile tool), Agile coach training, Agile & EVM, Release & Sprint Planning training and experience with Agile tools and techniques. | | | | | | |
| **LOE Hours** | Non Proj Spec – 11.2 | Phase 1  22.4 | Phase 2  33.6 | Phase 3  78.4 | Phase 4  302 | Phase 5  672 |
| *Meganoosh Avakian,* Senior QA Analyst | Computer Systems Analyst III | Ms. Avakian holds a Bachelors of Science degree and has her SHRM and ITIL certifications. She brings over 5 years of specialized experience working in Quality Assurance. Her qualifications include serving as a Senior QA specialist on the USDA PHIS program from 2014-2015 and her in-depth understanding of USDA requirements | | | | | | |
| **LOE Hours** | Non Proj Spec - 56 | Phase 1  168 | Phase 2  56 | Phase 3  33.6 | Phase 4  246.4 | Phase 5  280 |
| *Vijay Thottikkattu,* Software Engineering Manager / Solutions Architect | Project Lead – Application Systems and Programming III | Mr. Thottikkattu holds a Bachelors of Science degree in Elections and Communication Engineering and brings over 16 years of specialized experience in Information Technology. His qualifications include his experience working for USDA PHIS as a Development Manager and his in-depth knowledge of numerous technologies such as: C#, ASP.NET, VB.Net, ASP.NET MVC, LINQ, Entity Framework, WCF, and Oracle. | | | | | | |
| **LOE Hours** | Non Proj Spec – 11.2 | Phase 1  56 | Phase 2  224 | Phase 3  145.6 | Phase 4  560 | Phase 5  123.2 |
| *Kristina New,* Senior Business Analyst | Computer Systems Analyst II | Ms. New holds her MBA in Science, Technology and Innovation, a Masters degree in Electrical Engineering and a Bachelors degree in Computer Science. She has over 25 years of specialized experience in business analysis and program management for the Federal Government. Her other qualifications include excellent analytical skills and her ability to identify business process improvements that save time, money and improve quality. | | | | | | |
| **LOE** | Non Proj Spec - 56 | Phase 1  168 | Phase 2  593.6 | Phase 3  33.6 | Phase 4  224 | Phase 5  44.8 |
| *Bhaskar Nalluri*, Lead Developer (Software Team Lead) | Intranet / Intranet Application Specialist I | Ms. New holds her MBA in Science, Technology and Innovation, a Masters degree in Electrical Engineering and a Bachelors degree in Computer Science. She has over 25 years of specialized experience in business analysis and program management for the Federal Government. Her other qualifications include excellent analytical skills and her ability to identify business process improvements that save time, money and improve quality. | | | | | | |
| **LOE** | Non Proj Spec - 0 | Phase 1  106.4 | Phase 2  173.6 | Phase 3  145.6 | Phase 4  638.4 | Phase 5  56 |

## Staffing Plan

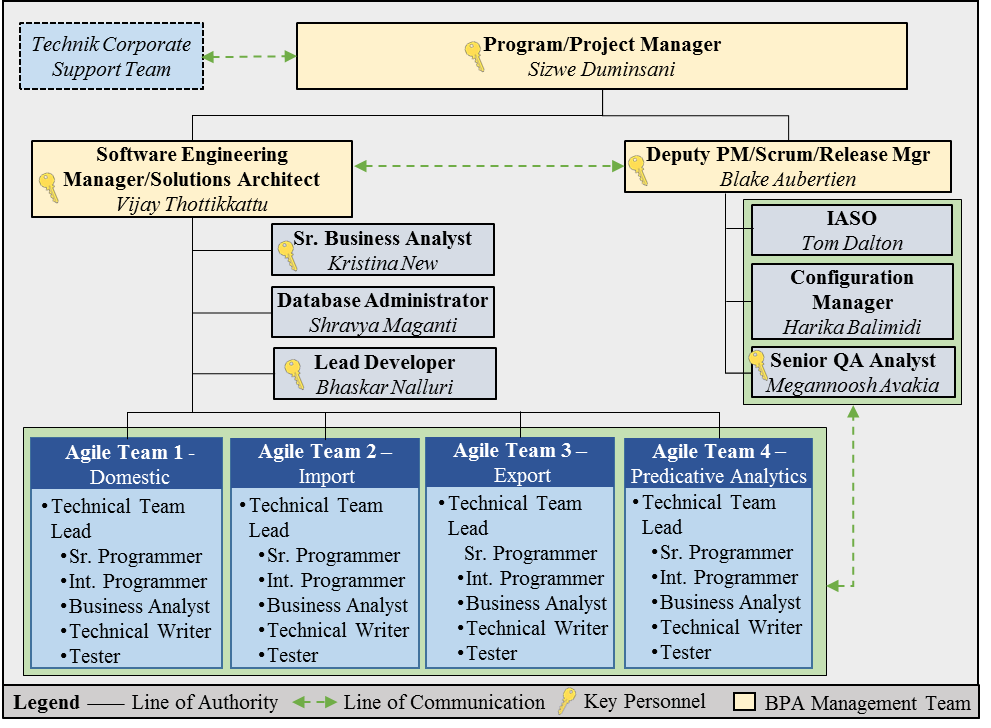
### Organization and Lines of Authority / Responsibility

To ensure continuity across multiple concurrent projects, we have established a BPA level organization structure, depicted in Figure X**Error! Reference source not found.**, which shows the staff and resources that will consistently support all projects. The figure shows “indirect” support functions in the top left box labeled as *Technik* Corporate Support Team. These individuals will provide critical support to the contract, but will not be billed directly to USDA.

Positions designated as “key personnel” are identified with a yellow key. A significant feature of our staffing approach is to establish competency-based teams, as illustrated in the bottom portion of the figure. An individual (*Technical Team Lead*) who is an expert in their field will lead each team. This collection of proposed key and essential staff (will play an instrumental role in planning, overseeing, and ensuring quality and consistency across each Task Order.

A second key feature of our staffing approach is the position of our Deputy PM/Scrum/Release Manager. Not only will Ms. Aubertein lend her project management expertise to help USDA PHIS achieve its objectives, she will also serve as the release manager for all tasks. This provides a fresh set of eyes reviewing each release and assuring that all products meet Technik’s high quality standards and all USDA expectations.

Our Program/Project Manager, Mr. Venkatesan, has the authority and autonomy to successfully lead the USDA PHIS effort. The lines of authority/responsibility in the figure below demonstrate the flow of authority on this effort; in addition, the lines of communication show other collaboration efforts and “reach-back” capabilities that will also occur to support USDA objectives.



### Staff Continuity and Ability to Back-Fill

Technik is committed retaining a workforce with the critical skills required to support the USDA PHIS effort. Technik recognizes that staff continuity is critically important for projects because turnover is expensive and top performers drive business performance. We utilize the following staff continuity strategy that allows staff to build a career, find mentors, and help them grow and develop while feeling more connected and engaged.

* **Recruit the right people in the first place.** Retaining top performers begins with hiring the right talent in the first place. Our recruiters leverage networking activities, staff referrals, job boards, and social media platforms to hire talented resources that possess the right combination of technical expertise and personality.
* **Listen to our people.** We use individual or group meetings to gain the insights and information to help us plan our retention strategy around areas most important and relevant to our staff.
* **Reward and recognize.** We strive to build our staff’s esteem. We value their opinion and ideas. We recognize staff members for their contributions and follow a policy that allows management to reward project staff after successful completion of a project.
* **Career development.** Career development strategies are planned for each staff member through their Individual Development Plans (IDP) and are aligned with each individual’s needs and desire for future growth. Our team provides continuous performance feedback to identify strengths as well as areas of improvement. We encourage our staff to maintain certifications by sending them to training and seminars.
* **Provide challenges.** Staff are given new job assignments to keep them alert and challenged. Providing staff with challenge and excitement encourages them to stay; they won’t want to risk missing a good opportunity.
* **Provide mentors.** We partner our staff with complementary skillsets together so both can benefit from the other person’s knowledge. Each staff member imparts technical skills and brings social and cultural lessons to the relationship.

Our recruitment, selection and back-fill process for this contract will include having candidates pre-screened, qualified, and available for any staffing need prior to the actual need. Our objective for this contract will be to populate a pipeline database so that we always have candidates pre-screened, qualified, and available for any staffing need prior to the actual need. For the PHIS contract, we will maintain a contract-specific database that matches only the profile of the PHIS projects skills and expertise. We will enter only the names of individuals who meet the qualifications of a particular labor category or who are experienced with the specific systems and applications in the client’s environment.

# Appendix 1: Resumes

## Project Manager, Satish Venkatesan

|  |  |
| --- | --- |
| **Position** | **Program/Project Manager** |
| **Legal Name** | **Satish Venkatesan** |
| **Education and Certifications** | * Masters in Computer Science * Bachelors in Engineering * Certified Project Management Professional (PMP) * Sun Certified Java Programmer * Microsoft Certified Professional |
| **Years of Exp** | 22+ |
| **Synopsis of Experience and Education/Training** | Mr. Venkatesan holds a Master's degree in Computer Science with over 15 years of Program Development and Project Management expertise. He has in-depth knowledge and experience in cost management, time management, risk management, and integration management. He is experienced in IT project budget analysis, outsourcing strategies, and contract management. He has strong technical background in systems architecture, database design, and network administration. He has proven ability to deliver high quality IT products and services on schedule and under budget. He has mitigated program risks that directly impact the realization of benefits He has led the organization to achieve ISO 9001:2008 certification for professional services and CMMI Maturity Level 3 (Version 1.3) Certification for Development (DEV) and Services (SVC). |
| **Technical Qualifications** | * Operating Systems: Windows 2003, Windows 2000, XP, NT, Windows 95, Linux * Languages: VB.NET, ASP.Net, C#, VB, C++, Java, C, VB, PowerBuilder, Win 32, MFC, VB Script, JavaScript, Active Server scripts * Databases: Oracle V6.x- 98.x, SQL Server 2000/7.x/6.x, SYBASE ASE/ASA, Ultralite * Software: .NET Technologies (ASP.NET, .NET Compact Framework etc) Metrowerks Code Warrior (6.x, 7.x, 8.x), embedded Visual Basic, embedded VC, ScoutBuilder, Satellite forms, JDK, Internet Information Server, Visual Interdev, Active Server Pages(ASP), Windows API |
| **Availability** | Mr. Venkatesan is available immediately to commence work on this project after award. |
| **Work Experience** | |
| **Technik, Inc.**  8/2008 to Present  **Project Manager**  *Project: USDA / APHIS – Digital Signature Pilot; VSPS Software Development & Support; Import and Export; NAIS Allocator Enhancements; NAIS Reporting, NAIS PSP; Websphere Portal Direction* | In this Project Management role, he has implemented a structured project methodology which includes: project definition, approval and communication, systematic project / risk controls, performance measurements and executive level reporting and metrics to the USDA Management Team. He used his expertise in designing and delivering Earned Value Management Systems (EVMS) reports including designing WBS, setting up Baseline Budget Control accounts, and work measurement by control accounts according to the PMI PMBOK guidelines. He has developed project schedule has and project management plans. He provides weekly status reports and monthly In Progress Reviews (IPR) which include all technical, schedules, and cost information as well as a summary of technical progress on items deemed of interest by VS project managers. The reports also contain a summary of all task activities, problems encountered, corrective actions taken, anticipated activity for the next reporting period, current month cost by hours, and dollars, an estimate of next month’s cost by hours and dollars, and finally the cumulative cost by hours and dollars since inception and any other items subsequently negotiated and approved by either the COTR or Contracting Officer. |
| **Project Manager**  *Project: US Department of Education, Office of Elementary and Secondary Education, Impact Aid System Support* | As the Project Manager for the Impact Aid Program, Mr. Venkatesan oversees the maintenance and enhancement activities for several IAS components. He monitors project progress and ensures that all work for DoE is compliant with the DoE IT security policy requirements, as well as FISM, OMB, HSPD and NIST standards and guidance. Additional project management activities include conducting kick-off meetings, progress meetings, monthly and quarterly progress reporting, contractor management plan, quality control plan, and emergency/ disaster contingency plan. |
| **Project Manager**  *Project: Securities and Exchange Commission – IT Support Services; Software Development Services; CorpFin Legacy Applications Maintenance* | As Project Manager, Mr. Venkatesan developed and maintained project schedules for software development activities and provided weekly progress updates. Developed and submitted a project schedule detailing the task timelines, milestones and delivery dates, weekly progress reports that covered work completed during the reporting period and status of milestones and work planned for the subsequent reporting period. Participated in weekly status meetings to estimate project status and conduct Project Risk management by reviewing the Issues and Actions recorded from the previous meetings and recording Issues or Actions that may have emerged during the new review period. |
| **Program Manager**  *Project: NASA, Information Technology Support Services* | As Program Manager, Mr. Venkatesan collaborates with the Technik Managing Director (MD) and NASA Senior Manager to develop contract-level performance goals, strategies to achieve these goals, and the metrics to quantify and report on these performance goals. He assists the MD identify ways to improve and/or redesign processes to achieve increased efficiencies and higher levels of customer satisfaction. |
| **Project Manager**  *Project: Department of Veteran Affairs, Innovation Applications – Daily Plan Web; Auto Order Standing Sentry System; Poppies Development; Spinal Cord Injuries Disorder Outcome* | In this Project Management role, he was in charge of a Performance Based Task Order for the Department of Veteran Affairs (VA). His team provided contractor support to develop, deploy and maintain multiple VHA Innovations Applications. He used his expertise in designing Earned Value Management Systems (EVMS) including designing WBS, setting up Baseline Budget Control accounts, and work measurement by control accounts and followed PMI PMBOK guidelines.  Mr. Venkatesan was is in charge of developing and maintaining task execution schedules, developing and planning resource assignments and allocations, conducting and analyzing program earned value performance and quality metrics, submitting program status reports, program reviews, and other project documentation, managing, tracking, and monitoring program deliverables, developing and maintaining the Project Management Plan and coordinating program logistics with the COTR. |
| **Project Manager**  *Project: Department of Navy, Financial Management Systems* | In this role, Mr. Venkatesan implemented a structured project methodology which included: systematic project controls and performance measurements; executive level reporting and metrics. He established program management controls to allow for timely impact analysis and benefits reassessment throughout the program. He identified and managed cross-project dependencies and resolved conflicting priorities. He identified and mitigated program risks that directly impact the realization of benefits. He participated in business and strategic planning sessions to ensure project alignment with organizational goals and priorities. |
| **Program Manager**  *Project: Navy Seaport – E Contract and Task Orders* | Created Project Plans, WBS, project resource assignments, resource hours, projected task completion dates and coordinated user acceptance testing activities |
| **Project Manager**  *Project: Department of Veteran Affairs, Electronic Certification Automatic Processing (ECAP)* | In this Project Management role, he was in charge of a Performance Based Work for the Department of Veteran Affairs (VA). His team supported the analysis, design, development, maintenance and support of Education Claims processing for VA. He implemented a structured project methodology, which included risk controls, performance measurements and executive level metric reporting. He developed Earned Value Management reports; set up Baseline Budget Control accounts. He worked extensively with the Technical team and chaired the Configuration Change Control Board. |
| **Project Manager**  *Project: Fairfax County Public Schools Project* | In this role, he enforced Quality assurance (QA) activities and assisted with baselining architectures. Developed Configuration Management plans and authored Standard Operating Procedures for Document Management (DM). |
| **Practice Area Manager, Program Manager, Consulting Manager**  *Project: United States Department of Agriculture- Veterinary Services (AQES – Automated Quarantine Examination Application)* | Acted as the Program Manager and Technical Architect in developing and deploying the AQES POCKETPC application for USDA. Performed all aspects of Project Management including developing project plans and milestone schedules. |

## Senior Business Analyst, Kristina New

|  |  |
| --- | --- |
| **Position** | **Senior Business Analyst** |
| **Legal Name** | **Kristina New** |
| **Education and Certifications** | * Bachelors of Computer Science * Masters in Electrical Engineering * MBA – Science, Technology and Innovation |
| **Years of Exp** | 25+ |
| **Synopsis of Experience and Education/Training** | Ms. New has extensive experience in program management, business analysis, technical writing and testing for the Federal Government. She is responsible for developing and managing efficient processes resulting in increased business and excellent customer service. She possesses excellent project management skills, analytical analysis, oral and written skills addressing business process improvements that save time, money and improve quality. She has extensive experience with RFPs, RFQs and federal procurement methods as well as contracting, software development and new business development. |
| **Technical Qualifications** | * Enterprise software licensing * IT Program Management * Department of Defense/Federal Procurement * Proposal responses for Federal/Commercial RFPs * Large Account Management * Small business development, sales & marketing * Technical Writing/Requirements Analysis * Search Engine Optimization |
| **Availability** | Ms. New is available immediately to commence work on this project after award. |
| **Work Experience** | |
| **Technik, Inc.**  10/2010 – Present  **Business Analyst**  *Project: Department of Education, Impact Aid System* | Ms. New was responsible for requirements analysis for new technical requirements that emerge in response to congressional mandates, technical updates and user experience improvements for the Department of Education's Impact Aid System (IAS). Ms. New conducted technical review meetings, documented requirements, and developed a testing environment with Oracle, completed unit and system testing, documented test procedures, updated project schedules and maintained communication with the customer as an assistant project manager for all software update deliveries and task orders. She analyzed both the business process and technical requirements for the Impact Aid System. Ms. New was responsible for requirements traceability, managing the development of the user interface and ensuring all requirements are incorporated in the development effort. She identified and coordinated risks associated with the project and supplied risk mitigation for requirements that were being refined to meet customer objectives. |
| **Business Analyst**  *Project: Department of Veterans Affairs, Office of Research and Development / Innovations* | As a Business Analyst for the Veteran Affairs, she has met with IT departments; gathered, analyzed, applied the IDEF0 model, and documented processes in the form of a Business Process Analysis (BPA) for the VHA Office of Research and Development (ORD). She has developed documents such as: Business Requirements Document (BRD), Test Cases, Traceability Matrices, and Release Notes in support of the requirements for the VA National Center for Patient Safety on its ‘The Daily Web’ application. She has expertise in gathering, interpreting, and reporting on operational data from IT programs, researching new technologies, creating assessment and preparing life cycle management documents in support of Veteran Affairs ORD information technology initiatives. |
| **Business Analyst**  *Project: Department of Veterans Affairs, IVMH* | As was the Business Analyst for the Improve Veteran Mental Health (IVMH) Analysis project, Ms. New was responsible for developing the interface document and requirements traceability for the Behavioral Health Lab (BHL) software to VistA as well as the requirements for distribution of Mental Health Clinical Reminders. The analysis was conducted using the FURPS+approach as a method to gather and analyze the requisite data to thoroughly document the key interface information from the business managers, Subject Matter Experts, archives and technical documents. All the requirements were documented according to the PMAS mandates including Business Rules, Usability Specifications, Applicable Standards and Interfaces. Ms. New was responsible for updating the Project Plan, manage risks and action items, authoring Monthly Progress Reports and Weekly Meeting Minutes, conducting analysis meetings and workshops and ensuring all deliverables were completed on time and correctly. |
| **Business Analyst**  *Project: US Navy* | Responsible for creating and delivering all documents associated with the Navy Budget Office BOATS program including Requirements, Design, Test and User Guides. Utilized Team Foundation Server and SharePoint to track development and documentation in compliance with CMMI procedures. Participated in business and technical analysis to determine and refine user requirements. |

## Deputy Project Manager/Agile Coach, Blair Aubertien

|  |  |
| --- | --- |
| **Proposed Position** | **Deputy Project Manager/Agile Coach** |
| **Legal Name** | **Blake Aubertien** |
| **Education and Certifications** | Bachelors of Science in Integrated Science and Technology |
| **Years of Exp.** | 15+ |
| **Synopsis of Experience and Education/Training** | Ms. Aubertien holds a Bachelor’s of Science degree and brings 15 years of experience as a highly talented project/program manager, Agile Coach and SME with extensive technical background in: requirements gathering, process definition, agile development methodology, systems analysis, design, testing, system integration and operation; significant experience in security and access controls; expertise in all phases of project delivery. |
| **Technical Qualifications** | PMP-ACP Preparation, Rally (Agile tool), Agile Coach Training, Jenkins, Tivoli, Siebel, Portal, Documentum, Jira (Agile tool), Test Director, SOA, WinRunner,Clarify-CRM, UNIX, ClearQuest, ClearCase, WebSphere Business Modeler, HP OpenView, MicroMuse Netcool, RSA SecureID, SharePoint, Checkpoint FW/VPN, CiscoWorks, Cisco Enterprise Management Solutions, Sun Solaris System Administration, Visio, Ensemble, Vantive Trouble Ticket, Peoplesoft FMS/HCM, Citrix, Lotus Notes, Microsoft Office Suite, Keys to Leadership, Agile & EVM, Release & Sprint Planning, Agile Tools & Techniques |
| **Availability** | Ms. Aubertien is available immediately to commence work on this project after award. |
| **Work Experience** | |
| **ABA Solutions**  6/2010 - Present  **IT Project Manager** | Ms. Aubertien assisted the US Citizenship and Immigration Service in its multi-year transformation to move from a paper based, benefit centric organization to an electronic, person centric organization providing real time tracking, viewing and status of immigration benefits as well as lead the federal government in its move from standard SDLC to Agile. Core to this transition is the design and development of a complex IT system to replace multiple disparate and aging IT systems used by the agency while supporting, adhering to and applying federal regulations. She assisted the program in laying the groundwork around project planning activities in a lean agile environment for both Scrum and Kanban and redefining the method for the development of requirements definition, design, test in support of transforming the organization while ensuring testability and business acceptance on a scalable level. She also was responsible for coaching in agile principles and practices in support of ELIS across multiple teams in agile principles and practices including iteration/sprint planning, backlog prioritization, user story writing, estimating user stories, relative sizing, developing acceptance criteria and conducting retrospectives as individuals transformed their thinking and approach to become a self-organized functioning agile team. She led brown bag training sessions and retrospectives for other teams who were transitioning to Agile with an emphasis on processes and practices that best embraced the USCIS Agile Culture; including continuous integration, test driven development, release and sprint planning, planning poker, backlog grooming, Acceptance Criteria, Definition of Done, User Story creation and Scrum of Scrums. |
| **Three Pillar Global**  2/2010 – 6/2010  **Lean Agile IT Project Manager** | Ms. Aubertien successfully assisted a client on a short-term effort to transform their custom GPS fleet tracking software application to better support an expanding customer base. She was responsible for coaching and using Agile project methodology to manage a fast pace transformation from scope definition through launch while managing the customer relationship. She facilitated workshops to examine the business rules and logic applied in the underlying code to develop a strategic plan for the projects software redesign objective. She worked with clients to gather system requirements and business rules, supporting Unit and QA testing by providing technical guidance on the impact of the system changes. She also managed the daily project activities and development team as they consolidated code into Web Service API’s to optimize performance and reliability using Extreme Programming techniques. |
| **Focus Technology**  10/2008-3/2009; 9/2009-2-2010  **IT Program Manager** | Ms. Aubertien was responsible for the timely and cost-effective management and delivery of a variety of large, concurrent projects within the IT Program Management Office. She directed the successful implementation of the Integrated Customer Portal project to refocus, with a customer centric philosophy and provide automated billing and customer account information within a central customer portal. She led the Enterprise Service Integrated Portal project in support of transforming the manual process of managing and maintaining customer networks, into an automated self-service application. She worked with IT and the business, leading them through the first major SDLC project introducing a hybrid Agile methodology to the organization. She managed the design, development, and revision of project schedules and budget; worked with IT, the business and outside vendors on project priority, scope and delivery. She also led teams through detailed requirements definition including: capturing business processes by developing use cases and field level data requirements. She developed communication documents and effectively communicated with key stakeholders and the project team members providing them with updates in a timely manner. She served as a liaison between the vendors, TekSystems and Sapient, development and business to ensure the traceability of delivery results, as per the user requirements in a global environment and she served as a SME for the Business Services .Net applications within the Program Management Office. |
| **Sprint Nextel Corporation**  12/2006-7/2008  **Sr. Project Manager/SME** | Ms. Aubertien managed full SDLC enterprise transform program from initiation through delivery, to implement systems and tools for all sales channels in support of the Sprint and Nextel merger. She led a global disperse program team responsible for a large-scale cross-divisional program, designated as top enterprise priority. She supervised project scope definition, planned major project phases, and established project success factors. She determined appropriate resource levels for projects. Managed projects through development, validation, launch, and post-launch assuring that projects met predefined goals and objectives. She represented sales organization on cross-functional teams rapidly implementing an integrated business systems platform in support of the merger and multiple new products. She interfaced with team, peers, vendors, and executives for the delivery of status, communications, impact and risk assessments, and sharing of best practices. She also acted as a Release SME during design reviews, training and testing development, security implementation and launch |
| **Fannie Mae**  4/2006-11/2006  **Sr. Technical Risk Specialist** | Ms. Aubertien served as a team lead in the ESM Risk Management Office for the following areas: Change Management, Problem Management, User Access (RAM, SOL, ADAMS), LDAP and Active Directory and a technical expert for Access Management controls. She managed team members during daily activities including test development, preparation, execution, and reporting in compliance with Sarbanes-Oxley regulations. She also interfaced with the Sarbanes-Oxley Executive team and ESM platform and process owners to ensure alignment and execution of infrastructure general computer controls (GCC) testing. She developed new testing approach based on enterprise level procedures across Change Management (ELSIF), Access Control and Logging & Monitoring and assisted platform owners with internal risk assessments of current business processes, identified control deficiencies and provided recommendations for remediation. She performed gap analysis of cross-departmental processes and procedures based on regulatory requirements. She also executed and conducted QA analysis of the operating effectiveness testing, extract and analyze data from multiple sources on business requirements and infrastructure problems; documented, reported, and communicated these to the Sarbanes-Oxley Regulatory Affairs PMO and business. |
| **Sprint Nextel Communications, Inc.**  10/2004-4/2006  **IT Manager** | Ms. Aubertien managed administration of User Access Control and Identity Management for over 33 different systems across multiple departments. She served as a SME on Sarbanes Oxley Regulations as the company transformed its operations to meet government regulatory compliance in a matrix organization. She also supervised a team of nine analysts tasked with providing internal customer service and system administrator support within three functional areas. Ms. Aubertien identified and assessed short-term and long-term program goals and coordinated work efforts with all groups that support application issue tracking and resolution. She assisted in defining the new corporate policies, processes and procedures for User Access and Identity Management to comply with Sarbanes Oxley Regulations. She also served as a SME for Identity Management providing technical guidance across the organization. She oversaw the maintenance of twelve Sarbanes-Oxley regulatory compliant production environments (i.e., identified risks and system controls, participated in monthly internal audits, bi-annually worked with external auditors to provide testing support, developed and executed remediation plans based on identified risks). She led weekly team meetings and provided regular feedback based on performance goals and career development plans and was responsible for contracting relationships, staffing and budgeting. |
| **UAT Security**  4/2003-10/2004  **IT Manager** | Ms. Aubertien was responsible for requirements definition and goal setting, project planning, identification and securing of appropriate resources. (Promoted from Sr. QA Analyst). She guided team members in career development and performance management goals. She managed analysts to work closely with business owners to gather and define requirements for security changes based on LOE assessments; translation of high-level to functional requirements and performed system impact or risk analysis for Executive Change Request Board. She performed process analysis on the impact of design changes within each release and ensured all documentation updates and provided technical leadership and guidance to security testing process; oversaw project team QA functions. She created end user procedural documentation defining step-by-step implementation of changes in production. Throughout lifecycle, Ms. Aubertien created and maintained relationships with internal business owners/users, provided technical and professional guidance to staff, tracked and monitored project progress to ensure on-time delivery. She assisted in defining and setting up users in a new implementation of the CRM tool, Clarify, as part of a customer relationship management initiative. She also managed all interim deliverables, work delegation, complex information analysis and development and presentation of security change recommendations. |
| **Ernst & Young**  8/1999-4/2003  **Senior Consultant** | Ms. Aubertien directed broad range of project functions related to diverse assignments in private industry for a global leader in management consulting and IT services. Led teams of 4-8 professionals in all phases of project development, from initial planning to post-production support and end-user training.   * Held key role in pre-planning (interfacing with clients to gather requirements, define business rules and develop scope), and worked closely with clients (ensuring on-target deliverables within budget) to develop business processes and procedures in support of post release operations. * As primary liaison, partnered with various disciplines to address issues to full resolution and client satisfaction. * Trained, mentored, and motivated new consultants to top performance. * Developed and monitored project schedules, facilitated activities to ensure projects are completed within schedule and satisfied business and requirements. * Managed team resources, staffing issues and individual performance evaluations.   **QA Project Manager, Nextel**  Led project team assigned to the Billing System Overhaul project for Amdocs’ Ensemble. Ensured software package met client’s requirements and interfaced with existing functionality. Managed On-line UAT team using UAT calendars and executing all test cases through Test Director. Reported project status to both Nextel and CGEY management.   * Managed team resources providing technical guidance, responsible for individual performance reviews and staffing issues. * Responsible for daily executive level reporting and managing issues for both front-end and back-end testing teams. * Analyzed functionality to ensure client’s requirements and business objectives were met. * Developed a regression-testing plan that encompasses all modules of Ensemble (CSM, Billing, A/R, Collections, Inventory Control, Price Plan, Security, MPS/EMS). * Managed testing of all front-end functionality of Ensemble. * Ensured resolution of all front-end issues/defects obtaining clear and accurate resolution from vendor. * Responsible for the adherence to the projected budget: managed billable vs. non-billable hours related to over-all expenditure of project budget; provided status reports to management regarding expenditures.   **Sr. Systems Analyst, Nextel**  Worked on a project team assigned to an enterprise level transformation project to overhaul the Customer Billing Systems.   * Met with business owners to define profile capabilities based on business rules/roles, to develop system level functionality within the Ensemble Security User Module. * Managed metrics to support system conversion and defect tracking for daily status meeting to Senior Management. * Oversaw resources to develop and configure Ensemble Security including, detailing and streamlining processes used to create ID’s with an automated solution. * Managed Security War room during conversion production support, including acting as the liaison between the project team and operations. * Created process and procedural documentation used in support of User Access operations post launch.   **Sr. Security Analyst, Teleglobe Data Center Development**  Assisted in the implementation and integration of security applications and documented security processes around business operations in to support an IDC (Internet Data Center).   * Made security recommendations and developed the enterprise security policies to govern network access for the Internet Data Center based on requirements gathering. * Managed vendor relationships, tool evaluations and selection. * Led the installation and configuration of SecurID User Authentication and Checkpoint Firewall/VPN. * Supervised the integration of new security tools with the network monitoring tool HP overview. * Created and delivered weekly team status to account executives.   **Network Architect, Charter Communications Network Operations Center**  Network Architect for the design of NOC technical architecture and support strategy for the management of all digital services for a Top “5” national broadband cable provider. Worked from a “green-field” environment to  design a network management solution to encompass all potential services, including cable-TV/digital-cable infrastructure, data-over-cable, VoIP and WebTV offerings.   * Responsible for EMS technologies, NOC infrastructure * Worked with business users to gather data and define requirements for NSOC tool selection. * Developed bill of materials and negotiated vendor hardware and software pricing and procurement for all NSOC equipment. * Responsible for installation, configuration, documentation and troubleshooting of server, hardware and software. * Created process and procedural documentation for business operations within the NOC including standard operational interactions down to ticket level routing. As well as developed and delivered training material to NSOC personnel.   **Project Manager, Bell South**  Project Manager for BellSouth’s project teams developing new products for entry into the long distance market. Responsibilities included: resolution of high-level issues escalated from product development; preparation of weekly status presentation updates to client executives; development of processes for reporting and communications; tracking of issues, risks, assumptions, and scope changes into the client program; and research of regulatory issues. |

## Quality Assurance Lead, Meganoosh Avakian

|  |  |
| --- | --- |
| **Proposed Position** | **Quality Assurance Lead** |
| **Legal Name** | **Meganoosh Avakian** |
| **Education and Certifications** | Bachelors of Science; Management  SHRM Certification – 2011  ITIL Foundation Certification; Information Technology - 2015 |
| **Years of Exp.** | 5+ |
| **Synopsis of Experience and Education/Training** | Ms. Avakian has 5+ years of experience in the IT field working as Quality Assurance Specialist. Her testing experience covers testing Web-based Applications in various industries using software development life cycle (SDLC), Waterfall and Agile Methodologies.  Her ability to effectively communicate with key stakeholders within both the Federal Government and Private industry has resulted in the timely successful completion of projects and contract renewals.  She has extensive experience with User Acceptance Testing and reporting protocols that provide required deliverables to management and clients. She has the ability to quickly master new functional requirements, workflows, system processes, and technologies when business logic requires it. She delivers critical thinking skills and logic-based approach when solving problems during Regression, Functional, Performance and UAT Testing. |
| **Technical Qualifications** | TFS/Visual Studio Ultimate, Test Manager, LoadRunner, QC/ALM, QTP (UFT),JIRA, SQL Server 2008,  Oracle, MS Report Builder, Crystal Reports, MS Project, MS Visio, Selenium, Salesforce, Windows,  Unix, VMWare, SharePoint, XML, .NET, C#, JAVA, MS Office Suite (Word, Excel, PowerPoint, Publisher, Access, Outlook) |
| **Availability** | Ms. Avakian is available immediately to commence work on this project after award. |
| **Work Experience** | |
| **KT Consulting**  6/2015 - Present  **Software Test Engineer** | Ms. Avakian is currently working as a software test engineer for KT consulting. She works on a team to provide services to the Centers for Medicare and Medicaid Services division. She tests Microsoft SQL server databases using SQL opueries to validate test cases. She manages multiple priorities and projects simultaneiouysky and assists the development and quality assurance teams with debugging and replicating issues, She identified test case reusability, executed test runs, and validated actual versus expected results. She was also responsible for updating and executing the test scripts. |
| **USDA**  5/2014 – 6/2015  **Sr. Quality Assurance Specialist** | While working on the PHIS project, Ms. Avakian created weekly and monthly reports for management and stakeholders as project progresses and created, managed and tasked new processes for the QA Team in order to meet project deadlines. She oversaw the conduct manual, Smoke and Black Box software testing to validate application functionality in over eight Development and UAT environments and participated in peer reviews with developers, analysts, designers, technical writers and functional managers impacted by new development projects to ensure the test plan satisfied requirements. Ms. Avakian wrote SQL queries using MS SQL Server (RDBMS) such as Joins to perform backend testing required to validate test cases and created baseline scripts using Load Runner for load and stress testing. She used Team Foundation Server (TFS) to communicate software bugs, tasks, system change requests, review items and requirements and assisted with the implementation of automation using Coded UI in Visual Studio. She created new Test Data for development and the QA team as needed for valid test results and assisted with Tier 3 Application Help Desk support using Footprint tickets for management. She also checked Test 508 Compliance using manual testing, WAVE, Jaws and Dragon tools. |
| **Department of Energy**  3/2011 – 5/2014  **Quality Assurance Analyst** | Ms. Avakian was involved in writing Test Plans, Test Strategy, Test scripts and Test Scenarios from System Requirement specifications. She interacted and worked with business analyst and UAT teams to understand the data requirement for the testing to be performed and performed both Manual and Automated testing for Black box, Functional, Regression, Usability, Performance, Load, Stress and User Acceptance Testing. She used HP Quality Center to gather the test requirements based on design specifications documents and uploaded them into Quality Center and used Quality Center to communicate and coordinate software bug fixes, and change requests. Ms. Avakian developed Virtual user scripts using VuGen for various applications; performed Correlation, Data Parameterization and customization of scripts. She created Vuser scripts for Load and Performance testing to verify the Throughput Capacity, to ensure that performance meets or exceeds previous performance benchmarks using LoadRunner. |
| **SunTrust Bank**  1/2010 – 3/2011  **Analyst/Test Engineer** | As an analyst. Ms. Avakian took part in the peer review of the requirements and created documents for the project from high level concepts to understandable language. She was involved in developing Test plans and Test cases including detailed expected results. As Test Engineer, she identified test case reusability, executed test runs, and validated actual versus expected results. She was responsible for updating and executing the test script in Test Director and used QuickTest Professional to perform Automation Functional and Regression Test. She enhanced the QTP scripts by inserting VBScript functions and Checkpoints to check for Broken Links, Text, Table, XML and Images, and Synchronization Point. She designed and generated Reusable Test Scripts using QTP. She attended project Review meetings and discussed issues including the progress of the project with development, project teams and business groups and led the training process of the Application workflow for developers and UAT testers. |

## Software Engineering Manager/Solutions Architect, Vijay Thottikkattu

|  |  |
| --- | --- |
| **Proposed Position** | **Software Engineering Manager/Solutions Architect** |
| **Legal Name** | **Vijay Thottikkattu** |
| **Education and Certifications** | Bachelors of Science in Electronics and Communication Engineering |
| **Years of Exp.** | 16+ |
| **Synopsis of Experience and Education/Training** | Mr. Thottikkattu holds a Bachelor’s of Science degree and brings 16 years of experience in Information Technology, working for international organizations and Government Agencies like IMF, USDA, DC government, NYC Board of Education and top companies like CACI, NEC ,Dimension Data, RLI Insurance. Professional experience as a Development Manager, Architect, Team Leader, Senior Software Engineer and Developer. Around 14 years of experience in implementing .Net framework based solutions in medium to large enterprises. He is hardworking, team oriented, great attention to detail (both technical and aesthetic), exceptional problem solving abilities, excellent communication and interpersonal skills, interest, capacity to learn and adapt quickly and mentor junior staff. |
| **Technical Qualifications** | * C#, ASP.NET, VB.Net, ASP.NET MVC, LINQ, Entity Framework, WCF, ASP.NET Web API, AngularJS, Knockout JS, Breeze JS, JQuery, HTML, CSS, XML, XSLT, Java, JSP, EJB. * SQL Server 6.5-2012, Oracle, ODBC, T-SQL, SQL ETL using SSIS. * Visual Studio 2003-2013, IIS 6-7.5, XML Spy, SharePoint, IBM DataPower, Cruise Control. * Business Objects Reports, SQL reporting services, Crystal Reports 11 8.0/6.0/5.0/4.5. * Team Foundation Server, PVCS, Microsoft Project, Microsoft Visual Source Safe 6.0. * Load Runner, NUnit, FXCop. * Visual Studio tools for Office, Visual Basic Applications (VBA). |
| **Availability** | Mr. Thottikkattu is available immediately to commence work on this project after award. |
| **Work Experience** | |
| **International Monetary Fund**  3/2012-Present  **Technical Lead** | Mr. Thottikkattu led a team of developers during full SDLC and was responsible for gathering requirements, creating project plans for Integrated Collection System 2.0 version. He designed the User interface prototypes for approvals from the Client and followed Agile methodology for development process. He was responsible for implementing responsive web design using Model-View-ViewModel (MVVM) architecture pattern. He designed single page application (SPA) using AngularJS, Breeze, RequireJS which provides fluid user experience and database integration with entity framework on the server. He designed the Web API libraries with well-defined business and data access layers to communicate with the UI layer. He was responsible for User Acceptance Testing and Customer sign off. As part of this effort he worked with the quality assurance team for deployment of the applications and also change management of the application.  **Environment:** Windows 2008, MS-SQL Server 2012, WCF, Web API, .NET Framework 4.0/4.5, C#, ASP.NET, JQuery, AngularJS, Breeze, Entity Framework, LINQ, Visual Studio 2013, XML, XSLT, Microsoft Team Foundation Server. |
| **USDA – PHIS/FSIS**  3/2009-2/2013  **Technical Lead** | Mr. Thottikkattu led a team of developers as Software Architect/Development Lead for the PHIS project. He was involved in all phases of this project life cycle i.e. Requirements Gathering, Design, Development, Testing and Deployment. He designed the interface prototypes for approvals from the Client and designed all the WCF services like Domestic Inspection, Establishment Profile, Resource Management and Lab sampling. He developed web projects like Predictive Analytics, Lab Sampling etc and was involved in the design and development of USDA Meat labeling project (LSAS).  For the FSIS project Mr. Thottikkattu worked as a Software Architect to design the application from start. He coded and unit tested the following modules Roles, Permissions and Menus. He also developed the Administration module to maintain all the components involved and used ASP.NET MVC to develop the Administration module.  **Environment:** Windows 2008, MS-SQL Server 2008 R2, WCF, .NET Framework 3.5/4.0, C#,ASP.NET MVC, ASP.NET Webforms, JQuery, AngularJS, Telerik controls, LINQ, Visual Studio 2010, XML, XSLT, Microsoft Team Foundation Server. |
| **NEC America**  8/2008-2/2009  **Technical Lead** | Mr. Thottikkattu worked on this project as a Technical Lead. He was actively involved in the design of the optimized database. He designed the Classes and Attributes for the communication layer. He was involved in the full life cycle of this project (Analysis, Design, Implementation, Testing and Maintenance). He was involved in the design of application-security policy and used WCF as the communication layer. He developed .NET assemblies using C# for different modules and applied proper design patterns to ensure code reusability and abstraction. He used Microsoft Enterprise Library release for .NET 3.5 for accessing data, exception handling, and logging. Mr. Thottikkattu also wrote the stored procedures involved in data base access. The system was designed with stored procedures with no embedded SQL. The business logic was distributed between data and business layer to increase performance.  **Environment:** Windows 2003/ XP, MS-SQL Server 2005, WCF, .NET Framework 3.5, C#, XML, XSLT, SOAP Microsoft Visio Enterprise Edition, Microsoft Team Foundation Server. |
| **DC-OCTO**  7/2007-7/2008  **Technical Lead** | Mr. Thottikkattu worked on this project as a Technical Lead and was actively involved in the design of the optimized database. He designed the Intranet and Internet system architecture, Classes and Attributes for the whole system. He was involved in the full life cycle of this project (Analysis, Design, Implementation, Testing and Maintenance) and in the design of application-security policy. He implemented the .NET Framework with the usage of ASP.NET, XHTML, XML, XSL/XSLT, and CSS for front end. He also developed .NET assemblies using C# for different modules and applied proper design patterns to ensure code reusability and abstraction. He used ASP.NET AJAX 1.0 for responsive user interface and used Microsoft Enterprise Library release for .NET 2.0 for accessing data, exception handling, and logging.  **Environment:** Windows 2003, SQL Server 2005, .NET Framework 3.0, C#, XML Web Services, Merant Dimensions, XML, XSLT, SOAP, ASP.NET, ASP.NET AJAX 1.0, JavaScript, XHMTL and Microsoft Visio, Team Foundation Server. |
| **International Monetary Fund**  1/2005-7/2007  **Senior Developer** | As a Senior Developer Mr. Thottikkattu coded and unit tested all the main modules which included Dual Security Model, Download and upload modules. He actively participated in the redesign of web site for easy access of information in the website. He coded and unit tested the ICS Admin module, which is used to manage requests from different country correspondents. He designed the Internet system architecture, Classes and Attributes for the whole system and was involved in the full life cycle of this project (Analysis, Design, Implementation, Testing and Maintenance).  **Environment:** Windows 2003, MS-SQL Server 2000, .NET Framework 2.0, VB.NET, XML Web Services, Visual SourceSafe 6.0, XML, SOAP, ASP.NET, ASP.NET AJAX 1.0, JavaScript, XHMTL and Microsoft Visio |
| **Additional Development Experience** | * Senior Developer, RLI Insurance, Peoria, IL, 1/04 – 12/04, Project: Claims Management * Senior Developer, Dimension Data, New York City, NY, 9/03 – 12/03, Client: Volkswagen Credit (Volkswagen and Audi), Project: Payment Estimator and Administration tool * Developer /Senior Developer, ICP, New York City, NY, 2/1– 8/03, Client: ICP, Project: Strada (Business Process Management - BPM), Client: New York City Board of Education, Project: Galaxy (Budgeting system for schools and districts), Client: Administration of Child Services (ACS, New York City) | Project: Preventive Organization Management Information * Developer, Lifeminders.COM, Herndon, VA, 10/00 – 1/01, Project: Vendor Reporting Module | Project: Lifeminders Wallet * Developer, Cognizant Technology Solutions, India, 2/00 – 9/00, Client: Schwans, Marshalls, USA, Project: Issue Management System * Developer, Data Software Research Company (DSRC), India, 6/99 –2/00, Client: Cable and Wireless, London, UK, Project: Global Proposal Generator (GPG), Project: Consultant Tracking System |

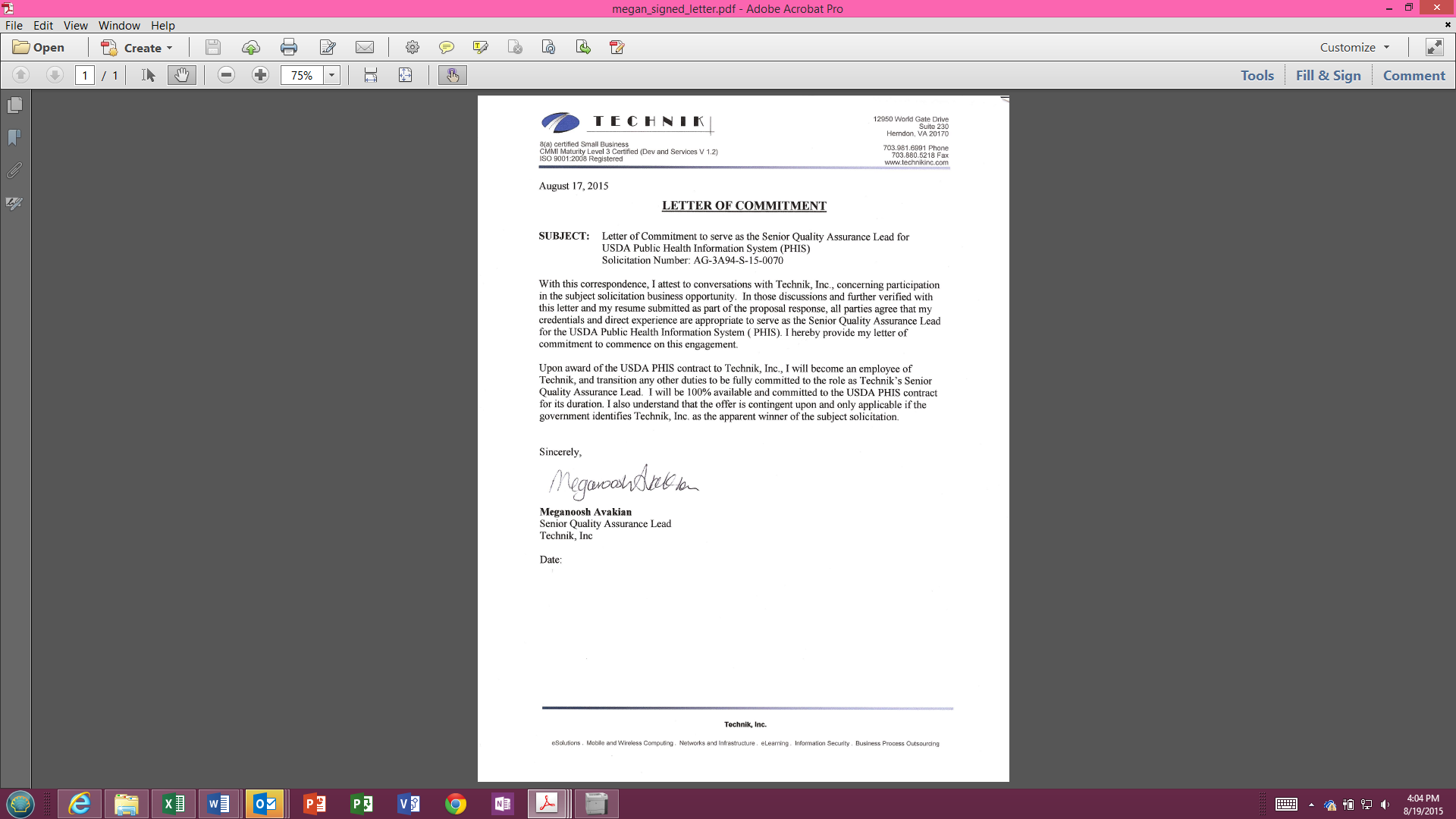
## Lead Developer, Bhaskar Nalluri

|  |  |
| --- | --- |
| **Proposed Position** | **Lead Developer** |
| **Legal Name** | **Bhaskar Nalluri** |
| **Education and Certifications** | Bachelors of Science and Technology, Computer Science and Engineering, JNTU  Microsoft Certified Technology Specialist (MCTS) |
| **Years of Exp.** | 13+ |
| **Synopsis of Experience and Education/Training** | Mr. Nalluri holds his Bachelors of Science degree in Computer Science and Engineering and has over 13 years of extensive experience with analyzing, designing, development, and maintenance of Internet, Intranet, Client Server and Object Oriented applications built on .NET Framework /ASP3.0/VB6.0. He has expertise in databases like SQL Server, Oracle & MS Access and developing web / client server reports using reporting tools such as Crystal Reports and Crystal web reports for .NET. Experienced in complete life cycle of the project and interacting with end users right from collecting requirements to Production Support. Experienced with software life cycle like Feasibility, System Studies, Design, Coding, Writing Test Cases, Implementation, Maintenance and End user Training. Reverse engineered & migrated various MS Access applications to [ASP.NET](http://asp.net/) web based applications for SEC. Reverse engineered the VB 6.0 COM components & re-written them in C# for better maintainability & re-usability in the previous projects. |
| **Technical Qualifications** | * Languages: C, C++, VC++, SQL, PL/SQL, Java * Databases/Technologies: MS-SQL Server, Oracle, Sybase, MS Access * GUI Tools: Visual studio. Net, Visual Studio, VSS * Front End Tools: Visual Studio 2005/2003, VB6.0 * Reporting Tool: Crystal Reports , Business Objects * Source Control: Visual Source Safe * Scripting Languages: VB Script, JavaScript, HTML, DHTML, CSS, XML/XSLT * Web Technologies: ASP.NET, ASP, C#. Net, VB.NET, MS Access, SharePoint, HTML * Web Server: Internet Information Server (IIS) * Operating Systems: Windows XP/2000/98/NT, MS-DOS * Knowledge: TFS (Team Foundation Server), Web parts, Integration Services, BizTalk Server 2004/2006, WCF, WPF, LINQ, MOSS 2007, WSS 3.0 * Microsoft Office: Access, Word, Excel, Outlook, PowerPoint, Project, Visio * Version Control: Serena Version Manager (VM), Team Track * Testing Tools: Bobby 508 |
| **Availability** | Mr. Nalluri is available immediately to commence work on this project after award. |
| **Work Experience** | |
| **Technik, Inc.**  10/2008-Present  **Software Engineer** | Mr. Nalluri participated in development, migration, production support enhancements for various web applications and MS access application. He developed and migrated various existing MS access applications to web based applications and reports. Application tasks include:   * COLD (Comment Letter Dissemination) – This web application is used for comment letter dissemination tracking. * Closing Memos – This web application is used to record the summary of filing reviews. * Reporting Applications – Online excel report generation for FACTS Reports, Division Reports, Division Dashboards, COLD Dashboards and Form D Reports * CF Intranet web site redesign – Redesigned for better usability * Emailing Comment Letters - Developed a secure process for Emailing Comment Letters * 508 Compliance – Updating various web application pages to 508 Compliance * Responsibilities include: * Design and Development of Web Forms Using ASP.NET & C#.Net. * Design of system process flow. * Design and development of the components for middle tier (Business Layer) Using C#.Net. * Development of Stored Procedures. * Development of XML Web services. * Create Linked Server to access Sybase tables in Sql Server. * Database Design   **Environment:** .NET Framework 3.5, XML, XPath, AJAX, C#.Net, Asp.Net, Sql Server 2005, Reporting Services, Integration Services, Sybase, MS Access, Windows XP/2003 |
| **Parish Soft LLC**  6/2008-9/2008  **Software Engineer** | Mr. Nalluri was involved in the Address Correction Process module of Online Church Management Software. The Address Correction Process is a semi-automated process through the USPS Address Management System using various utilities like AEC, ACS & CASS. Responsibilities included:   * Design and development of Web Forms Using ASP.NET & C#.Net. * Design of system process flow. * Development and configuration of Windows service for automated communication with USPS Secure website. * Design and development of Windows Forms Using C#.Net * Design and development of the components for middle tier (Business Layer) Using C#.Net. * Development of XML Web services. * Development of test-cases for the entire automated & manual process.   **Environment: .**NET Framework 2.0/3.5, XML, XPath, AJAX, C#.Net, Asp.Net, Web Services, Windows Service, Vss 6.0, Windows XP. |
| **AVL North America**  10/2008-Present  **Software Engineer** | Mr. Nalluri was involved in the various projects (Data Extractor, Data Integrator web services and Syntax parser). Data Extractor - This is windows application for data extraction from Java based GM internal web service. Extracted data from the GM web service stored as separate XML files in the AVL system. Data Integrator web service – This web service serves as a data provider system for various AVL applications. AVL applications accepts list of Serializable objects as input data. This web service uses the XML files extracted by Data Extractor and converts them into various Serializable objects depending on the request. Responsibilities included:   * Responsible for Design and Development of Web Forms Using ASP.NET & C#.Net. * Design and Development of Windows Forms Using C#.Net * Design and development of the components for middle tier (Business Layer) Using C#.Net. * Developed Reusable Classes using C#.Net. * Developed XML Web services. * Simulate the Java based Web Services into .Net Web service. * Improved the application performance using Memory management. * Developed Custom User Controls To reduce the Complexity in User Interface Coding and provide better look and feel. * Developed Test Cases for production system.   **Environment:** .NET Framework 2.0, XML,XPath,C#.Net, Asp.Net, Web Services, MS Excel, Vss 6.0, Windows XP/2000/2003 |
| **Ad-Insights**  4/2007-12/2007  **Software Engineer** | Mr. Nalluri worked as a software engineer on Ad-Insights. The purpose of Ad-Insights was to provide the most accurate and complete automotive advertising information in a timely and user-friendly manner to enable insightful marketing decisions. Users of this tool include Ford Motor Company Personnel (mainly in marketing); Ford’s marketing suppliers, and employees of all agencies of record working on Ford Motor Company business. Responsibilities included:   * Design and development of Web Forms Using ASP.NET & C#.Net. * Design and development of Windows Forms Using VB.Net. * Developed in Java Script for validating client side data entry web screens. * Design and development of the components for middle tier (Business Layer) Using C#.Net. * Developed Reusable Classes using C#.Net. * Developed Data Layer using ADO.NET to communicate with MS SQL Server. * Developed XML Web services. * Developed Client Server Applications using Remoting. * Improved the application performance using stored procedures and connection pooling and Memory management. * Database Schema Design using Entity Relational Modeling. * Developed Custom User Controls To reduce the Complexity in User Interface Coding and provide better look and feel. * Produced written Test Cases for production system.   **Environment:** .NET Framework 2.0, XML, SQL Server2000/2005, HTML, AJAX, JAVA Script, CSS, MS Excel, VSS 6.0, Windows XP/2000/2003. |
| **Old Mutual Financial Network**  4/2007-12/2007  **Software Engineer** | Mr. Nalluri worked on developing, enhancing and supporting various Web Based projects (Public portal, sales link portal). Web Based Systems were developed/ enhanced with service-oriented architecture using Asp.net, Vb.net, C#.Net, XML and Sql Server2000/2005. Responsibilities included:   * Gathering and Analyzing the Business Requirements. * Design and developed the database and Web pages. * Creating stored procedures, Views, Functions, Dynamic Sql, Cursors and T-Sql. * Developed Data Layer using ADO.NET to communicate with MS SQL Server. * Creating custom/User controls and master pages for reusability. * Developed reusable classes using OOP’s concepts in C#.net and Vb.Net. * Developed Reports using Reporting Services. * Developed various web services using XSD with WSCF (Web Services Contract First). * Java Script and Validator controls for validating client side and server side data entry web screens * Documentation of the each screen developed for the application * Involved in Database Design using Entity Relational Modeling. * Visual Source Safe was used for version control.   **Environment:** .NET Framework 1.1, .NET Framework 2.0, XML, SQL Server2000/2005, HTML, CSS, AJAX, JAVA Script, MS Excel, Vss 6.0, Windows XP/2000 |

## Letter of Commitment, Technik Employees



## Letter of Commitment, Meganoosh Avakian



# Appendix 2: Performance Work Statement

Quoters must provide a performance work statement (PWS) (Appendix # 2 of the technical quotation) outlining the activities/outcomes that will be accomplished by the quoter in order to satisfy the objectives outlined in the Statement of Objectives (SOO) (See Attachment #2 to solicitation) for the BPA task order. The PWS must use terms/phrases that require/obligate the contractor to fulfill the activities/outcomes. Examples of such terms/phrases include: “the contractor shall complete an analysis to determine …” “The contractor shall deliver a detailed list of…”

Quoters are expected to clearly demonstrate a thoughtful and unique approach for developing and executing task order 1. Proposed personnel must have considerable experience in system design and development. Quoters must propose the most effective methods for carrying out tasks described in the SOO. Quoters shall indicate how they propose to carry out all of the objectives and tasks and not merely repeat the language of the SOO.

Quoters may find it necessary to adjust the schedule provided in the SOO in accordance with the strategies, operations and procedures that they propose. In such a circumstance, quoters shall clearly identify any changes form the schedule laid out in the SOO and explain the rationale for these changes. Quoters should keep in mind that it is FSIS’s intent that the contractor move forward with all work as quickly as possible while maintaining the high quality of products and services.

The proposed plan must be written in enough detail that a review panel can adequately judge its full merits. Quoters should not expect the Government to make assumptions or guesses; quotations must be detailed and not vague.

## Introduction Section

This section introduces the parties (FSIS and contractor)

The United States Department of Agriculture (USDA) Food Safety and Inspection Service (FSIS) ensures that the Nation's commercial supply of meat, poultry, and egg products are safe, wholesome, and correctly labeled and packaged, as required by federal law. FSIS Public Health Information System (PHIS) was developed to collect, mine and analyze inspection, surveillance and investigative data, predict hazards and vulnerabilities, communicate or report analysis results and target resources to prevent or mitigate the risk of food borne illness and threats to the nation’s food supply.

## Background Section

This section elaborates on the background information surrounding the PHIS design and development requirements such as the objectives of the task order.

The Public Health Information System (PHIS) is a web-based software application that integrates and streamlines all scheduling, assigning, tracking, and documentation for FSIS’ tasks including import management, export management, domestic production inspections, and risk analysis. FSIS employees, representatives of countries with whom the United States maintains an import/export relationship, and meat, poultry and egg production establishments, which are subject to inspection may use PHIS. PHIS replaces several legacy client-server applications, automated multiple paper and email-based processes.

The PHIS Implementation Project has been divided into common Business Communities to define the team and affected primary users. The Business Communities are Domestic, Import, Export, Lab Sampling, and Predictive Analytics.

An alternative version of PHIS is available offline through the PHIS Disconnected State (DCU) program. Designed to work when broadband is unavailable; DCU allows the Consumer Safety Inspector, Enforcement Investigations and Analysis Officer and Auditor roles to perform many of the functions available online. Then, once Internet connectivity is available, upload changes through a synchronization process.

The PHIS is built on a Service Oriented Architecture (SOA) with re-usable components. The SOA is implemented with Service BUS Architecture and implements the reusable common services: Authorization Service, Logging Service, User Notification Service and Event Driven Architecture; reusable common components, a common user interface, and implements a Composite Applications (Portal). PHIS includes - SAS analytics environment with algorithms that analyze data and create models to detect patterns in disparate data. The PHIS also includes a SAP Business Objects Reporting environment.

## Scope of Work Section

Similar to an executive summary, this section provides an overview of the tasks to be completed.

The effort to be procured under this contract is to expand and develop new, when deemed necessary, functionality to support FSIS’s mission critical areas; Custom Border Control (CBP), domestic, import, export, and state inspection. Software defects, including all tasks and supplies necessary to perform concept definition and planning, development, modification/enhancements, implementation, support etc… and the associated Project Management of the contracted tasks to meet business needs and regulatory requirements—both existing requirements as well as those needs determined from gap analysis emerging during the contract period of performance. PHIS contract will evolve the As-Is system to eliminate or mitigate the As-Is system shortcomings. The design of these enhancements and fixes may require enhancements to the infrastructure, to include defining, designing, integrating, testing and deploying enhancements to the PHIS infrastructure. Project management encompasses the tasks necessary to manage and support all system development and application infrastructure deliveries. Security patching is mandated to be completed on all FSIS infrastructure servers, the contractor will be provided a testing schedule from FSIS OCIO and will be support by OCIO to complete patch testing to all PHIS servers. An analysis report of patch testing will be provided to OCIO Project Manager/ COR to address any issue with PHIS servers.

The objectives for the PHIS contract are detailed in the table below. The PWS tasks provided in *Section 9.4* are cross referenced with the PHIS objective number.

| **No.** | **PWS Area** | **PHIS OBJECTIVE** |
| --- | --- | --- |
| **1** | 1 | Specific enhancements and development will be to the four production modules. These enhancements and fixes will be established and managed using an FSIS prioritization process and a development “cost” estimation system to manage workload |
| **2** | 1 | Software defects, including all tasks and supplies necessary to perform analyses, development, testing and deployment delivery, and support and the associated Project Management of the contracted tasks |
| **3** | 1 | The design of enhancements and fixes may require enhancements to the infrastructure, to include defining, designing, integrating, testing and deploying enhancements to the PHIS infrastructure. Project management encompasses the tasks necessary to manage and support all system development and application infrastructure deliveries |
| **4** | 1 | Provide systems analysis, development, unit test, regression test, and deployment |
| **5** | 1 | This contract will address the PHIS Enhancements for the import, export, state, predictive analytics and domestic functionalities, reporting capabilities as well as current software defects |
| **6** | 1 | Implement, in partnership with the Government Program Manager, an approach to managing the PHIS program that: a) maximizes flexibility; b) significantly increases efficiency; c) Reduces Total Ownership Cost (RTOC); d) identifies and manages risk; e) and generates, maintains and uses near real time data. This management approach must support: Program Planning and Budgeting System (PPBS) process activities, flexible allocation of resources, identification of cost reduction initiatives |
| **7** | 1 | Incorporate a disciplined risk management process across all aspects of PHIS to facilitate attainment all program objectives. Risk identification, analysis and mitigation efforts will drive identification and reporting of key program metrics. Establish a modeling and simulation capability to manage key risk areas throughout the program to effectively reduce life-cycle cost, perform Cost As an Independent Variable (CAIV) trades, and mitigate schedule and performance risks |
| **8** | 1 | Manage PHIS Program to ensure efforts remain within cost and schedule. This management plan should describe the management processes the contractor has in place or plans to put in place to identify and track output-oriented metrics and tie them to cost data and program milestones. Data should come from existing processes the contractor currently uses to status programs, assess earned value and project EAC |
| **9** | 2 | Perform concept definition and planning, development, implementation on OFO Management Controls |
| **10** | 2 | Perform concept definition and planning, development, implementation on Supplier tracking/STEPS/Recall/TRECS |
| **11** | 2 | Perform concept definition and planning, development, implementation on Cooperative Interstate Shipment (CIS) |
| **12** | 2 | Perform enhancement on PHIS four modules |
| **13** | 2 | Perform concept definition and planning, development, implementation on new requirements approved by administrator |
| **14** |  | Support reporting capacity/report/alerts |
| **15** |  | Support browser/operating compatibility, testing and upgrade/testing for web; browser compatibility |
| **16** |  | Perform enhancements on CAVF/OEVP |
| **17** |  | Support for CBP connection/support for CBP interface connection |
| **18** |  | Support cross FSIS applications |
| **19** |  | Review of any unclosed FootPrints Tickets, SCRs and RFCs and provide solution |
| **20** |  | Review of all Team Foundation Server (TFS requirements for PHIS) |
| **21** |  | Provide description of system operations including schedule of operations |

## Tasks Section

Tasks and activities associated with the PHIS Design and Development contract are detailed in the following table. The PWS numerical designation has been cross referenced with the Statement of Objectives (SOO) numerical designation (see *Section 9.3, Table XX*) and the SOO Task Area (*SOO, Section C.6*).

| **PWS #** | **SOO Cross Ref** | **Tasks / Activities** |
| --- | --- | --- |
| **1** | **SOO Objective: 1, 2, 3, 9, 10, 11, 12, 13, 14, 15, 16**  **SOO Task Area: C.6.5, C.6.6, C.6.7, C.6.8, C.6.9, C.6.10, C.6.11, C.6.12** | **Application Development and Support** – The Contractor shall perform new development, enhancement and software defect tasks / activities in support of FSIS’s mission critical modules of:   * Export * Domestic * Imports * Supplier Tracker * Lab Sampling/Predictive Analytics * State Inspection (Export/Imports/OFO Management Controls/Cooperative Interstate Shipment) * Custom Border Control (CBC)   The Contractors provision of development tasks/activities may include new development and software defects, including all tasks and supplies necessary to perform concept definition and planning, development, modification/enhancements, implementation. The Contractor shall development and enhance all modules per the task order requirements listed in *PHIS Requirements FY 16-18.xlsx* (Attachment 3 of the solicitation).  The Contractor shall follow *FSIS Enterprise Performance Life Cycle (EPLC) / System Development Life Cycle (SDLC)* guidelines in the provision of full system lifecycle support in the execution of PHIS solutions and services. The Contractor shall adhere to the FSIS SDLC process and gates, which include: requirements analysis, design, development, integration and acceptance and associated milestones/deliverables. |
| **1.1** | **SOO Objective: 1, 6, 9, 10** | **EPLC Process of Planning –** The Contractor shalldefine the management parameters of the PHIS project and ensure that all the pre-requisites for delivery are in place. The Contractor shall develop and implement a partnership with the Government that : a) maximizes flexibility; b) significantly increases efficiency; c) Reduces Total Ownership Cost (RTOC); d) identifies and manages risk; e) and generates, maintains and uses near real time data. This management approach must support: Program Planning and Budgeting System (PPBS) process activities, flexible allocation of resources, identification of cost reduction initiatives. |
| **1.1.1** |  | **EPLC Planning Entry Criteria –** The Contractor shall meet all *Entry Criteria* before entering the Planning Phase.   * The Contractor shall obtain decision to proceed by the USDA Project Sponsor and/or Solution Owner * The Contractor shall ensure approval of final versions of all required deliverables from prior phase. |
| **1.1.2** |  | **EPLC Planning Phase Gate –** The Contractor shall complete all Exit Criteria prior to the PHIS project exiting the Planning Phase and entering the Delivery Phase, which includes the SDLC process of Requirements Analysis, Design, Development, and Integration/Acceptance.   * The Contractor shall complete, submit and obtain acceptance for all deliverables and baseline in the CM documentation library * The Contractor shall update business case (as needed) * The Contractor shall assign project resources, to include PM as key personnel * The Contractor shall initiate project change control and communication process * The Contractor shall establish project tracking and reporting processes |
| **1.1.3** |  | **EPLC Planning Phase Milestones and Deliverables** – The contractor shall complete all Planning Phase milestones and deliverables.   * **Public Release of Contract Documents** - The contractor agrees to submit, within ten workdays from the date of the CO’s execution of the initial TO, or any modification to the TO (exclusive of Saturdays, Sundays, and Federal holidays), a portable document format (PDF) file of the fully executed document with all proposed necessary redactions, including redactions of any trade secrets or any commercial or financial information that it believes to be privileged or confidential business information, for the purpose of public disclosure at the sole discretion of FSIS. The contractor agrees to provide a detailed written statement specifying the basis for each of its proposed redactions, including the applicable exemption under the Freedom of Information Act (FOIA), 5 U.S.C. § 552, and, in the case of FOIA Exemption 4, 5 U.S.C. § 552(b)(4), shall demonstrate why the information is considered to be a trade secret or commercial or financial information that is privileged or confidential. Information provided by the contractor in response to the contract requirement may itself be subject to disclosure under the FOIA. Submission of the proposed redactions constitutes concurrence of release under FOIA. * **Project Kick-Off** – The Contractor shall schedule and coordinate a Project Kick-Off within three (3) weeks of contract award. The meeting will provide an introduction between the Contractor and Government personnel who will be involved with this Contract. The meeting will provide the opportunity to discuss technical, management, and administrative issues and provide near term plan of action for getting each project underway. * **Project Management Plan (PMP)** – The PMP shall a) Describe the technical approach, organizational resources, and management controls to be employed to meet costs, performance and schedule requirements; b) Document planning assumptions and decisions; c) Document the schedules for each task activity; d) Identify the task order deliverables and deliverable dates for Government review and acceptance; and e) Develop a distribution list and deliverable format for all task order deliverables. * **Performance Management Plan** – The Contractor shall document the explicit job responsibilities, priorities and performance expectations of the project team. Further, the plan shall set forth the quality assurance process to be utilized by the contractor to ensure all tasks / artifacts are compliant with standards established by the contractor’s organization as supplemented by any specific quality requirements established in the contract * **Integrated Master Schedule (IMS)** – The Contractor shall develop and maintain in accordance with any applicable FSIS work breakdown structure, earned value, or other schedule standards a master schedule detailing the work, resources, and delivery dates for project deliverables. The project schedule shall be delivered MS Project format in soft copy and shall using the FSIS approved template and shall be provided no later than the contract kick-off session. * **Weekly Status Report** – The Contractor shall provide weekly status reports to the COR/COTR, detailing major accomplishments, upcoming tasks/activities, and possible delivery risks * **Monthly Progress Report** – The Contractor shall provide the COR, a report that provides valid and timely program status information to higher management. The report shall: a) Describe significant issues or issues requiring Government attention; b) Describe tasks accomplished this reporting period, task scheduled for completion that did not complete, task scheduled to start that did not start, and tasks scheduled for the next reporting period; c) Describe the accomplishments, problems/issues and present recommendation for corrective actions; d) Provide a summary of travel (includes travelers names, purpose, travel destination and cost) performed during any monthly reporting period, if applicable; and e) provide a self-assessment of contractor performance. * **Quarterly In-Progress Review (IPR) Session and Report** – The Contractor shall provide the COR, a report that provides valid and timely program status information to higher management. The report shall: a) Describe significant issues or issues requiring Government attention; b) Describe tasks accomplished this reporting period, task scheduled for completion that did not complete, task scheduled to start that did not start, and tasks scheduled for the next reporting period; c) Describe the accomplishments, problems/issues and present recommendation for corrective actions; d) Provide a summary of travel (includes travelers names, purpose, travel destination and cost) performed during any monthly reporting period, if applicable; and e) provide a self-assessment of contractor performance. The IPR Report shall be presented to an audience determined by the Government. A Monthly Progress Report will not be required in the month an IPR Report is due. The IPR Report will separately address the previous month’s events.   **Additional Task Management Deliverables –** The Contractor may be required to submit additional Task Management deliverables which include, but are not limited to:   * Project Work Plan with Work Breakdown Structure * Communication Plan * Quality Control Plan * Risk Analysis and Mitigation Plan * Configuration Management Plan * Security Plan * Project Performance Measurement Plan * Records Archival Plan * Disaster Recovery Plan * Communications and Marketing Plan Matrix * Telecommunications Plan * Certification and Accreditation Phase 1 * Cost Performance Report * Trip Report |
| **1.1** | **SOO Objective: 4** | **SDLC Requirements Analysis Phase –** The Contractor shall obtain a thorough and detailed understanding of the business need and break it down into discrete requirements, which are then clearly defined, reviewed, and agreed upon with the customers, decision-makers, and stakeholders. The objectives of this phase include:   * Complete all documentation identified in the project-specific Tailoring Plan for the Requirements Analysis Phase, along with the proper governance boards using the proper templates in the EPLC/SDLC Library * Define and baseline the business, functional, non-functional, and system requirements * Review the current and to be business process * Formally evaluate commercial products (as needed) as possible solutions to the business needs * Allow all business and systems areas impacted by the project to have the opportunity to participate in defining and/or reviewing the requirements from their respective areas of expertise |
| **1.1.1** |  | **Requirements Analysis Governance Reviews –** The Contractor shall conduct the following Governance reviews:   * **Preliminary Requirements Review (PRR)** – The Contractor shall conduct a review for reasonableness of selected work-in-progress requirements artifacts. The PRR is a review of work-in-progress documentation for the Requirements Analysis phase. It is a formalized milestone in the Project Management Plan (PMP) which provides a checkpoint for the PM and project sponsor to ensure that the Requirements Analysis Phase is on track. This mid-phase review ensures that the requirements documents are examined before end of the phase (40% completion), allowing sufficient time for course correction if needed. It is the PM’s responsibility to use this milestone to identify, raise, and take remedial action on any identified deficiencies with documentation. * **Critical Requirements Review (CRR)** – The Contractor shall conduct a thorough review of obligatory requirements artifacts. The CRR is a thorough, functional/non-functional requirements review based on the expectation that the Requirements Analysis is complete for the project. Because of this review, the project team may be required to correct and/or modify one or more deliverables before the project is allowed to proceed to the Design Phase. Feedback gathered in this review is used to correct the documentation where appropriate or can be documented for inclusion in subsequent System releases (or project iterations). The CRR milestone review ensures that all specified requirements artifacts are reviewed, and that the requirements are accepted by the proper governance authorities in the Program Area. As this is a critical milestone, it is necessary to get the explicit sign-off of the MDA (EMD ACIO, BAD ACIO , CSD ACIO, IAD ACIO, CTO, DCIO, CISO and CIO) at this review. The PM is responsible for ensuring that updates are completed and approved, in the CRR before going to the Requirements Phase Gate.  The CRR an Enterprise Management Division (EMD) Associate Chief Information Officer (ACIO) / Business Application Division (BAD) ACIO/ Chief Technology Officer (CTO) / Deputy CIO (DCIO) /CIO checkpoint. |
| **1.1.2** |  | **Requirements Analysis Phase Gate –** The Contractor shall complete all Exit Criteria prior to the PHIS project exiting the Requirements Analysis Phase and entering the SDLC Design Phase.   * The Contractor shall ensure that All required Requirements Analysis Phase deliverables completed, reviewed, and approved * The Contractor shall ensure that the CRR successfully passed * The Contractor shall ensure that all documentation is copied into the appropriate folder on the MS Project Server * The Contractor shall ensure that all required documents submitted to Configuration Management for control and storage |
| **1.1.3** |  | **Requirements Analysis Activities –** The Contractor may perform the following activities during the Requirements Analysis Phase.   * Further define and refine the functional and data requirements and document them in the Requirements Document. * Complete business process reengineering of the functions to be supported, e.g., verify what information drives the business process, what information is generated, who generates it, where does the information go, and who processes it. Suggest potential business process improvements that will result in greater efficiency and/or effectiveness in the business area. * Develop detailed data and process models including system inputs and outputs. Identify available data repositories existing in other systems/applications. * Develop the test and evaluation requirements that will be used to determine acceptable system performance. |
| **1.2** | **SOO Objective: 4** | **SDLC Design –** The Contractor shall create a technical solution that satisfies the functional requirements for the system by translating functional specifications into technical specifications. |
| **1.2.1** |  | **Design Governance Reviews –** The Contractor shall conduct the following Governance reviews:   * **Preliminary Design Review (PDR)** – The Contractor shall conduct a review of reasonableness for selected work-in-progress design artifacts. * **Critical Design Review (CDR)** – The Contractor shall conduct a thorough review of required design artifacts. It is an MDA Checkpoint. |
| **1.2.2** |  | **Design Phase Gate** – Permits exit of project from Design and entry into the Development phase. |
| **1.2.3** |  | **Design Milestone and Deliverables –** The contractor shall complete all System Design Phase milestones and deliverables.   * Concept of Operation Document * Technical Architecture/Flow Document * System Design * Requirements -Traceability Matrix * Software Requirements List * Hardware Requirements List * Network Requirements List * Network Modeling / Bandwidth Usage Estimates |
| **1.3** | **SOO Objective: 4** | **SDLC Development Phase-** The Contractor shall conduct build and validate the new system as specified in the Design phase to the point that it can be turned over for Acceptance. The objectives of this phase include:   * Complete all documentation identified in the project-specific Tailoring Plan for the Development Phase, with the proper governance boards identified in the Deliverables Spreadsheet using the proper templates in the EPLC/SDLC Library * Develop the infrastructure and applications to achieve the user’s requirements * Prepare all documentation for business users, systems operations and support groups |
| **1.3.1** |  | **Development Phase Entry Criteria –** The Contractor shall meet all *Entry Criteria* before entering the Development Phase.   * Design Phase Gate sign-off has occurred * High-level Design document approved * Detailed System Design document approved |
| **1.3.2** |  | **Development Phase Governance Reviews –** The Contractor shall conduct the following Governance reviews:   * **Test Readiness Review (TRR)** – The Contractor shall conduct an assessment of the code-complete and developer-tested system’s readiness for independent testing. |
| **1.3.3** |  | **Development Phase Gate –** The Contractor shall complete all Exit Criteria prior to the PHIS project exiting the Development Phase and entering the Integration/Acceptance phase.   * All required Phase Deliverables completed, reviewed and approved; * Integration Test completed and results approved; * All governance milestones successfully passed; * Infrastructure is integrated and operational within the developer’s environment; and * All required deliverables submitted to Configuration Management for control and storage. |
| **1.3.4** |  | **Development Phase Activities –** The Contractor may perform the following activities during the Development Phase.   * Code programs, modules and scripts * A full walk-through the code of every program, module, and script * Perform the Technical Architecture (TA) Compliance Audit process to ensure that the defined technical architecture of the system is compliant with the FSIS Technical Architecture (FSIS TA) * Perform unit testing of programs, modules and scripts and document results of those test * Perform and obtain approval of the Integration Test Plan * Perform the integration testing of the system based on the Integration Test Plan * Develop, review and test the Installation/Back-out Instructions. If instructions already exist, create an addendum with the new instructions, and attach to the existing instructions * Prepare and obtain approval of the Integration Test Plan * Write or modify and review the user manual(s) * Write or modify and review the user training materials * Write or modify and review Operations manual using the template * Write or modify and review Support manual and scripts. * Conduct the Test Readiness Review (TRR) * Follow the CM process to submit code and documentation to CM * Update Project Plan and Business Case * Update the Requirements Traceability Matrix (RTM) * Review any previously approved documents that have been updated during this phase during Governance Reviews * Obtain approval of requirements and close the analysis phase * Submit approved documentation to Configuration Management |
| **1.3.5** |  | **Development Milestone and Deliverables –** The contractor shall complete all Development Phase milestones and deliverables.   * Business Scenario Script * Data Warehouse Application - Deployment Plan for Development Environment |
| **1.4** | **SOO Objective: 4** | **Testing Phase –** The Contractor shall ensure validation of PHIS software and system components that have been developed or modified. The Contractor shall be responsible for unit and string testing before the software is approved for full testing. The Contractor shall also be responsible for debugging and correcting defects under this contract. Test efforts identify bugs, integration and performance issues, and validate that the software meets user and system requirements. Test Efforts perform testing on software in all stages of the life cycle, including newly developed systems, existing systems that have been enhanced, and software that has had bug fixes and routine and emergency maintenance modifications. The following contracts apply to the Testing Phase:   * Multiple environments with different testing stages and purposes will be present in the USDA Enterprise Data Center (EDC), allowing simultaneous testing of one or multiple systems at different stages of the testing/validation life cycle. * The Contractor shall work with FSIS to obtain managed access to these environments. * PHIS will not be the only system in the test environment and coordination with the COR will be required. * Automated test scripts are mandatory for the PHIS and shall be written and verified in accordance with FSIS compliance and used during all PHIS system and integration testing. * Infrastructure: A review of the infrastructure supporting PHIS will be done, and recommendations to improve performance and security provided to PHIS. * Defects: Software defects in the production system are managed in the FSIS Numera Footprints ticketing system. Issues will be identified, triaged, and addressed as prioritized by FSIS. |
| **1.4.1** |  | **System Testing –** The Contractor shall perform system testing, to include system integration, integration testing, and regression testing. System Test efforts ensure the system operates as designed without defects in the production environment. The Contractor shall provide test procedures and automated test scripts for each enhancement and fix, installation instructions, and evidence of successful verification and validation. System test requirements include:   * The Contractor shall plan and conduct verification tests. The Contractor shall communicate the plan and schedule of these quality measures. The Contractor shall report to FSIS, as part of its weekly progress reporting, the status and results of reviews and tests, including associated risks, issues, and plans to mitigate and/or rectify contributing factors. * The Contractor shall coordinate updates to existing work products and work products created within this System Test Services task with FSIS. In addition to provide test plan, RFC and all documents needed to pre-production team for testing. |
| **1.4.2** |  | **Acceptance Testing –** The Contractor shall perform Acceptance Test efforts, demonstrating to Stakeholders that the application addresses all business requirements and implements the agreed-upon design and enhancements in a workable manner. This includes 2 subtasks Functional Test and User Acceptance Test. Functional Test Services include rigorous regression testing or exception testing, and ensure that the system has been fully exercised and meets functional and performance requirements. UAT Services shall be performed to provide end users with a hands-on opportunity to assess and accept the overall functionality and interoperability of the entire system. |
| **1.4.3** |  | **Acceptance Testing Assistance to Testers** – The contractor shall assist the COR with facilitating independent verification and validation by FSIS or parties designated by COR. The contractor shall assist the COR facilitating testing by FSIS users as well as volunteers from the FSIS business partner community. This includes configuring test IDs, explaining test scripts, assisting users who encounter problems and compiling and verifying tester results. Test results and planned corrections are reported to the COR during each weekly test cycle. Test environment should be accessible to necessary FSIS personnel to test enhancements, fixes, or general functionality in various roles as defined by PHIS. |
| **1.4.4** |  | **Performance and Stress Testing –** The Contractor shall perform comprehensive performance and stress testing as needed to verify enhancements and fixes comply with the PHIS performance requirements. Performance testing may vary given the type, size, and scope of the PHIS Release. Performance and stress testing shall include, as appropriate, the following elements:   * Database volumes * Transaction volumes * Concurrent user logons * Concurrent activities and load balancing * Batch transaction volumes (daily and other cycles) * Batch processing windows and dependencies (daily and other cycles) * Response time expectations * Network (public and private) load considerations * System interfaces and printing * Other performance tests appropriate to the type, scope, and size of the software/system product, as specified in the Task Order SOW. The Contractor shall modify system and software products to rectify deficiencies in the system identified during testing. The Contractor shall coordinate with FSIS to produce updates to existing work products, including those created within this Performance and Stress Test effort.   The contractor shall test and report results to the COR that detail how tests were conducted and how the test results validate that the application meets FSIS and USDA performance requirements under test conditions that mirror or simulate those in production. |
| **1.4.5** |  | **Testing Milestone and Deliverables –** The contractor shall complete all Testing Phase milestones and deliverables.   * Usability Testing * Usability Test Results Matrix * System Test Procedures/Plan * System Test * User Acceptance Test Scripts * Test Data * Test Results Matrix |
| **1.5** | **SOO Objective: 4** | **SDLC Integration /Acceptance Phase-** The Contractor shall ensure that every aspect of the application being developed along with any supporting data conversion routines and system utilities are thoroughly validated by the Stakeholders prior to proceeding with Implementation. The Contractor shall update all supporting documentation and reference materials to ensure consistency with the deployed system. Objectives of the Integration/Acceptance Phase include:   * Complete all documentation identified in the Project-Specific Tailoring Plan for the Development Phase, with the proper Governance Boards using the proper templates in the EPLC/SDLC Library * Conduct a system test that ensures the system meets its requirements * Prioritize resolution of identified problems – and pursue resolution if needed – before production installation * Conduct Systems Operations and Technical Services training before deployment * Perform a user acceptance test (UAT) and document the results * Finalize and obtain approval of all business user, Systems Operations, and Technical Services documentation before deployment |
| **1.5.1** |  | **Integration /Acceptance Phase Entry Criteria –** The Contractor shall meet all *Entry Criteria* before entering the Integration /Acceptance Phase.   * Development Phase Gate sign-off has occurred |
| **1.5.2** |  | **Integration /Acceptance Phase Governance Reviews –** The Contractor shall conduct the following Governance reviews:   * Release Readiness Review (RRR) – The RRR milestone review ensures that all specified requirements artifacts are reviewed, and that the requirements are accepted by the Program Area. As this is a critical milestone, it is necessary to get explicit sign-off from the MDA (EMD ACIO, BAD ACIO, CSD ACIO, IAD ACIO, CTO, DCIO, CISO, and CIO). |
| **1.5.3** |  | **Integration /Acceptance Phase Gate –** The Contractor shall complete all Exit Criteria prior to the PHIS project exiting the Integration /Acceptance Phase. This marks the end of the SDLC.   * All Phase Deliverables completed, reviewed and approved * System Test results approved * User Acceptance Test Results approved * All phase deliverables submitted to Configuration Management for control and storage   Unlike prior Phase Gates where the PMB Chief made the go/no-go decision, the MDA exercises gating authority at the RRR. Only the MDA has authority to release Systems into production.  The MDA is provided with all RRR deliverables. Based on these inputs, the MDA decides whether or not the project passes its Integration/Acceptance Phase Gate. No project may continue to deployment without an affirmative decision from the MDA. |
| **1.5.4** |  | **Integration /Acceptance Phase Activities –** This phase consists of the following processes, most of which are responsibilities of the Agency’s Independent Test and Enterprise Data Center (EDC) Test Lab O&M teams. Guidance in this section is provided to illustrate important interactions among deliverables.   * Install system in test environment and test the installation/back-out procedures * Perform system testing to validate the system against design and requirements. During the testing, the development team is available to resolve any problems * Conduct training sessions with Systems Operations and Technical Services personnel * Update all business user, Systems Operations, Support Services, and Technical Services documentation as needed based upon testing performed to ensure that documentation matches the actual system * Conduct the UAT and obtain approval of results. After user sign-off, Production Support must be notified and must receive a copy of the user documentation for reference * Update the Project Plan and Business Case * Update the Requirements Traceability Matrix (RTM) |
| **1.7** |  | **Deployment Milestone and Deliverables –** The contractor shall complete all Deployment Phase milestones and deliverables.   * Updated User Guide and Mapping Matrix * Online and Live Training * Operations and Governance Plans * Data Warehouse Application - Deployment Plan |
| **1.8** |  | **Maintenance and Support Milestone and Deliverables –** The contractor shall complete all Maintenance and Support Phase milestones and deliverables.   * O&M - Knowledge Transfer Session 1 * O&M - Knowledge Transfer Session 2 * O&M - Knowledge Transfer Session 3 * Updated Application Enhancement Matrix * Project Management Lessons Learned |
| **1.8** |  | **Training Support and User Guide Development or Revision** – Although Contractor does not perform training, The Contractor shall develop materials for and provide technical assistance to those who perform training in the use of the system and in its use in the business context. The Contractor shall be responsible for describing/presenting new functionality to designated groups based on COR requirements. |
| **2** | **SOO Task Area: C.6.11** | **Support Services –** The Contractor shall provide support services to include**:**   * **Infrastructure Support** – The design of enhancements and fixes may require enhancements to the infrastructure, to include defining, designing, integrating, testing and deploying enhancements to the PHIS infrastructure. * **Security Patching** – Security patching is mandated to be completed on all FSIS infrastructure servers, The Contractor shall be provided a testing schedule from FSIS OCIO and will be support by OCIO to complete patch testing to all PHIS servers. An analysis report of patch testing will be provided to OCIO Project Manager/ COR to address any issue with PHIS servers. * **Resolve Bugs** – The Contractor shall resolve bugs/issues & CCB according to SDLC. The contractor shall develop/enhance all approved work includes modifications to the system based on the recommendations made by the PHIS Change Control Board (CCB) or new policy/legislative mandates. |
| **3** | **SOO Task Area: C.6.4** | **Transition to Support -** The Contractor shall successfully support transition to FSIS PMO with no break in level of support. Tasks include:   * The Contractor shall turn over all documentation, information and knowledge to the Government, allowing the PMO to support the FSIS/PHIS application and it’s associated projects. * The Contractor shall conduct weekly training session to ensure uninterrupted performance of FSIS/PHIS applications. * The Contractor shall confirm to FSIS that identified staff receive the knowledge and skills needed to maintain all programs the contractor has designed, maintained, tested and implemented. * The Contractor shall review key components of FSIS/PHIS Projects with the Government. * The Contractor shall mentor the assigned FSIS staff in the development of the skills needed to perform this scope of work. * The Contractor shall develop a draft Transition Plan (TP) that describes the management of Task 4, Transition to Support activities. The Contractor shall submit this draft TP to the Government within fifteen (15) business days after the Governments request. The Contractors TP will detail Contractor resources and roles involved in the transfer; detail weekly training sessions; provide a list of risks and mitigation strategies for the transfer; and contain a detailed resource balanced project schedule developed with Microsoft Project. * The Contractor shall meet with the FSIS bi-weekly (twice a month) to discuss the progress and status of the knowledge transfer. The Contractor shall submit an updated MS Project Schedule during this meetings, as well as discuss any risks or concerns. |
| **4** | **SOO Objective: 3, 6** | **Task Order Management** |
| **4.1** | **SOO Task Area: C.6.1** | **Orientation Briefing** - The Contractor shall conduct an orientation briefing within 10 business days of task order award. This Briefing will initiate the communication process between the Government and the Contractor and ensure a common understanding of the task order requirements and objectives. The Contractor shall document the meeting minutes and submit and electronic copy to the COR within five (5) days of the Orientation Briefing. The Contractor’s Quality Control Plan will be submitted to the COR for review within 20 days of the Orientation Briefing |
| **4.2** |  | **Government Furnished Property** - The Contractor shall manage (control, use, report as required, preserve, protect, repair and maintain) all Government Furnished Property (GFP) in its possession. |
| **4.3** |  | **Security** - The Contractor shall assign a Security Officer to oversee all security activities and ensure compliance with Federal and USDA mandates, directives, policies and procedures. |
| **4.4** | **SOO Task Area: C.6.2** | **Knowledge Transfer / Transition In**- The Contractor shall perform Knowledge Transfer activities within an approximate one-hundred seven (107) day time frame and deliver a draft and final Knowledge Transfer Plan (KTP) to the Government. The Contractor shall develop and submit a Knowledge Transfer Plan (KTP) within 15 days of task order award. The Contractor shall attend weekly status meeting with the Government in order to maintain effective communication with the outgoing Contractor and Government personnel. The Contractor shall meet with the FSIS bi-weekly (twice a month) to discuss the progress and status of the knowledge transfer. The Contractor shall submit an updated MS Project Schedule during this meetings, as well as discuss any risks or concerns. |
| **4.5** |  | **Project Schedule** – The Contractor shall develop, update and submit a Project Schedule detailed to a level such that no tasks has a duration of more than ten (10) working days. The project schedule will identify tasks, dependencies, deliverables and milestones. The Project Schedule will be baselined and updated continually throughout the period of performance. |
| **4.6** |  | **Balanced Scorecard -** The Contractor shall develop a strategic management and measurement system that links the task objectives to a comprehensive range of key performance indicators. The Contractor shall convert labor categories and associated labor rates to dollars and plot this information in graph format as part of the scorecard. |
| **4.7** | **SOO Task Area: C.6.3** | **Period Of Performance Summary Report** – The Contractor shall provide an accurate, up-to-date description of work performance and accepted for the Base and Option Year Periods of Performance; and ad-hoc, as requested by the Government. |
| **4.8** | **SOO Objective: 7** | **Risk Management –** The Contractor shall develop and execute aRisk Management Plan which details the process of identifying, assessing, responding to, monitoring, and reporting risks. This Risk Management Plan defines how risks associated with the enterprise systems architecture, engineering, development and integration support services project will be identified, analyzed, and managed. It outlines how risk management activities will be performed, recorded, and monitored throughout the lifecycle of the project and provides templates and practices for recording and prioritizing risks. The Contractor shall provide timely notification to the COR/COTR when programmatic or project based risks are evident. |
| **4.9** | **This PWS area supports all objectives** | **Quality Assurance -** The Contractor shall be solely responsible for the supervision, management, and inspection of its employees under this PWS. The Contractor shall monitor and ensure its employees meet the requirements of this PWS. The Contractor shall provide and maintain an inspection system acceptable to the Government covering deliverables/services provided under this PWS. The Contractor shall develop and submit to the government a Quality Control Plan (deliverable). |
| **4.10** | **SOO Objective: 17, 18, 19, 20, 21** | **Transition Out –** The Contractor shall develop and submit a Transition Out Plan at the Kick-Off meeting (deliverable). The Contractor shall submit an updated Transition Plan the COR at least 15 days prior to the transition period beginning, if the incumbent contractor is not the follow-on contract awardee. The Transition Plan shall describe how The Contractor shall provide a seamless transition to a successor that does not impact FSIS operations. The Plan shall address the following areas:   * Review of any unclosed FootPrints Tickets, SCRs and RFCs; * Review of all Team Foundation Server (TFS requirements for PHIS) * Description of program office requirements that have not yet been implemented as well as an estimate of the resources needed to complete them; * Description of system operations including schedule of operations; * Review and description of eCert and CBP requirements and configurations * Description of reengineering opportunities * Detailed summary as well as work papers and files for work that is in progress. * Explanation of ongoing issues, how they are being dealt with, options and long-range plans; * Update to all requirements, design documents and plans * Any current security issues raised by the contractor or for which the contractor has supported fact finding; and * The known status of any ongoing reviews by outside parties including CIO, independent C&A reviewer, IV&V reviewer, OIG, or GAO. * Knowledge Transfer Sessions at the outgoing/in coming vendor locations and government sites * Must have Key Personnel for outgoing and incoming transition to be staff during the 60-90 transition: Senior Business Analyses , Project Manager, Team lead Developers, Team lead Technical writes, Senior Quality Assurance Analysis * Senior Application Program, Senior Configuration Management, Software Architect Information system Auditor for outgoing and incoming vendors |

## Delivery Schedule Section

This section elaborates on the date in which each proposed deliverable/service will be rendered to the Department.

All deliverables will be submitted electronically by email and removable electronic media, as well as placing in FSIS’ designated repository (either FSIS’ Project Server or Share Point document management tool, to be discussed at kick-off). Electronic formats will adhere to the following compatibility requirements.

* Text – MS Word
* Spreadsheets – MS Excel
* Briefings – MS PowerPoint
* Drawings – MS Visio
* Schedules – MS Project

All deliverables shall reference the order number and project number. Both numbers can be located on the award documents provided to the offeror. The project number will begin with “PMO-XX-XXX-Project Name, where “XX” is replaced with the project fiscal year, “XXX” is replaced with the project’s unique identier for that fiscal year, and “Project Name” is replaced with the project’s title.

| **Deliverable / Milestone Name** | **Submission Date** |
| --- | --- |
| **Non Project Specific** | |
| Public Release of Contract Documents | Within 10 workdays from the date of the CO’s execution of the initial TO, or any modification to the TO. |
| Weekly Status Report | Once/week on Tuesday |
| Balanced Scorecard | Once/week on Tuesday |
| Monthly Progress and EVM Report | Once/month |
| **Phase 1 – Project Planning** | |
| Project Kick-Off Meeting | Once, within two weeks of award |
| Project Management Plan – Draft | NLT 5 workdays after Kick-Off Meeting and then yearly |
| Project Management Plan – Comments | 5 workdays after Government receipt |
| Project Management Plan – Final | 10 workdays after receipt of Government comments |
| Project Work Plan with Work Breakdown Structure | First iteration during this phase, with updates as required throughout project |
| Communication Plan | First iteration during this phase, with updates as required throughout project |
| QCP – Draft | Within 20 days of Kick-Off |
| QCP – Comments | 5 workdays after Government receipt |
| QCP – Final | 10 workdays after receipt of Government comments |
| Risk Analysis and Mitigation Plan | First iteration during this phase, with updates as required throughout project |
| Configuration Management Plan | First iteration during this phase, with updates as required throughout project |
| Security Plan | First iteration during this phase, with updates as required throughout project |
| Project Performance Measurement Plan | First iteration during this phase, with updates as required throughout project |
| Records Archival Plan | First iteration during this phase, with updates as required throughout project |
| Disaster Recovery Plan | First iteration during this phase, with updates as required throughout project |
| Communications and Marketing Plan Matrix | First iteration during this phase, with updates as required throughout project |
| Telecommunications Plan | First iteration during this phase, with updates as required throughout project |
| Certification and Accreditation Phase 1 | First iteration during this phase, with updates as required |
| **Phase 2 – System Design** | |
| Concept of Operation Document | First iteration during this phase, with updates as required |
| Technical Architecture/Flow Document | First iteration during this phase, with updates as required |
| System Design | First iteration during this phase, with updates as required |
| Requirements -Traceability Matrix | First iteration during this phase, with updates as required |
| Software Requirements List | First iteration during this phase, with updates as |
| Hardware Requirements List | First iteration during this phase, with updates as required |
| Network Requirements List | First iteration during this phase, with updates as required |
| Network Modeling / Bandwidth Usage Estimates | First iteration during this phase, with updates as required |
| **Phase 3 - Development** | |
| Business Scenario Script | First iteration during this phase, with updates as required |
| Data Warehouse Application - Deployment Plan for Development Environment | First iteration during this phase, with updates as required |
| **Phase 4 - Testing** | |
| Usability Testing | First iteration during this phase, with updates as required |
| Usability Test Results Matrix | First iteration during this phase, with updates as required |
| System Test Procedures/Plan | First iteration during this phase, with updates as required |
| System Test | First iteration during this phase, with updates as required |
| User Acceptance Test Scripts | First iteration during this phase, with updates as required |
| Test Data | First iteration during this phase, with updates as required |
| Test Results Matrix | First iteration during this phase, with updates as required |
| **Phase 5 - Deployment** | |
| Updated User Guide and Mapping Matrix | First iteration during this phase, with updates as required |
| Online and Live Training | First iteration during this phase, with updates as required |
| Operations and Governance Plans | First iteration during this phase, with updates as required |
| Data Warehouse Application - Deployment Plan | Once at any point during this phase |
| **Phase 6 – Maintenance and Support** | |
| O&M - Knowledge Transfer Session 1 | Once at any point during this phase |
| O&M - Knowledge Transfer Session 2 | Once at any point during this phase |
| O&M - Knowledge Transfer Session 3 | Once at any point during this phase |
| Updated Application Enhancement Matrix | Once at any point during this phase |
| Project Management Lessons Learned | First iteration during this phase, with updates as required |

## Performance Standards Section

This section provides a performance standard in which FSIS will use to judge success/failure of each proposed service/deliverable.

## Assumptions Section

This section clearly delineates any performance assumptions supporting the proposed tasks. This section should NOT include technical or business/pricing assumptions that are traditionally posed in the business/technical volume.

## Constraints Section

This section elaborates on the operating constraints in which the quoter expects to perform the tasks.

## Government Furnished Equipment Section

This section clearly outlines any Government furnished equipment that must be rendered to the contractor in order to enable the completion of the proposed services/deliverables.

The Contractor shall manage (control, use, report as required, preserve, protect, repair and maintain) all Government Furnished Property (GFP) in its possession. GFP is defined by the Government and Technik as “property in the possession of, or directly acquired by, the Government and subsequently made available to the Contractor”. The Contractor shall initiate and maintain the processes, systems, procedures, records, and methodologies necessary for effective control of GFP, consistent with standards and/or industry-leading practices and standards for GFP management. The Contractor’s responsibility extends from the initial acquisition and receipt of GFP, through stewardship, custody, and use until formally relieved of responsibility by authorized means. This includes delivery, consumption, expending, sale (as surplus property), or other disposition, or via a completed investigation, evaluation, and final determination for lost, stolen, damaged, or destroyed property, and applies to all GFP under the Contractors accountability, stewardship, possession or control.

## Government Furnished Information Section

This section clearly outlines any Government furnished Information that must be rendered to the contractor in order to enable the completion of the proposed services/deliverables.

All contractors will be appropriately vetted according to USDA policies (including background checks/NACIs or clearances) and are required to complete security awareness training before being provided system access. Where appropriate, contractors will be required to sign a non- disclosure agreement as a condition of the contract.

## Place of Performance Section

This section states the place of performance. It should be noted that, due to certain objectives, the place of performance is expected to be variable.

Performance will take place primarily at Technik offices, located at 12601 Worldgate Drive, Suite 230, Herndon, VA 20170.

Project personnel will work onsite at USDA when necessary. 1400 Independence Ave. SW

Washington D.C. 20250

# Appendix 3: Compliance Matrix

| **Section L: Instruction Quotation Instructions** | **Proposal Page & Paragraph** |
| --- | --- |
| **Section 1- Abstract/ Table of Contents** - A two-page summary should be provided abstracting the quotation contents in language understandable to a layperson. The abstract shall indicate full acceptance of the solicitation requirements or specify any exception. |  |
| **Section 2- Technical Approach – BPA set up** - The quoter shall provide a narrative response which demonstrates an understanding and comprehension of the requirements described in the BPA Statement of Work (SOW) (attachment  #1), as well as any inherent problems or obstacles associated with the objectives of this procurement. |  |
| **Section 2- Technical Approach – BPA set up** - The quoter shall also address its understanding of the mission and objectives of FSIS and PHIS. |  |
| **Section 2- Technical Approach – BPA set up** - The technical approach should also include a staffing plan (including labor categories) consistent with the technical approach to the overall BPA, including identifying the services needed and identification of any critical issues including risk identification and mitigation. |  |
| **Section 2- Technical Approach – BPA set up** - If subcontractors are proposed, the quoter shall describe the efforts to be performed by the prime and the subcontractor(s), along with rationale describing the division of responsibilities and benefits of these arrangements to the Government. |  |
| **Section 2- Technical Approach – BPA set up** - The quoter must be CMMI level 3 or above certified, and must provide the certification as an appendix (4) in order to be considered for award. |  |
| **Section 3- Technical Work Plan – BPA task order -** In the Technical Work Plan, quoter’s shall fully detail and explain the strategies, operations and procedures that they propose to fulfill the tasks outlined in their proposed PWS. |  |
| **Section 3- Technical Work Plan – BPA task order –** The quoter should organize, by task, the descriptions of work to be performed and the methods to be used. Each task should be presented under a separate heading with the same numerical designations as presented in the proposed PWS and mapped to the objectives outlined in the Statement Of Objectives (SOO) (attachment #2). The Technical Work Plan should present detailed information on how the quoter plans to accomplish the tasks proposed in the quoter’s proposed PWS. |  |
| **Section 3- Technical Work Plan – BPA task order –** Included in the Technical Work Plan should be a project plan, outlining and detailing the projected dates and deliverables to be provided in accomplishing the task. |  |
| **Section 4 – Corporate Experience –** The quoter shall elaborate on its recent corporate experience (along with any major subcontractors) providing services that are similar in size, scope and complexity to the solicited requirements. The contractor shall provide a list of at least three (3) but no more than five (5) relevant contracts. |  |
| **Section 5 – Past Performance –** In order to facilitate the Government’s evaluation of the contractor’s past performance, the contractor shall submit a past performance questionnaire to each of the references listed in the “Corporate Experience” section of the technical quote. |  |
| **Section 6 –** Quoters shall present a Management Plan showing the strategies for implementing their proposed technical work plan through administrative structures and operating procedures to successfully carry out each task. |  |
| **Section 6 -** Quoters shall explain how they propose to manage and coordinate operations and personnel working for the contractor, including any subcontractors and consultants, as well as the quoter’s employees. |  |
| **Section 6 -** Details of quality control and cost containment efforts- including for any awarded option periods – are critical to the effort and must be included. |  |
| **Section 7 – Personnel, Qualifications, and Staffing -** The quoter should provide personnel that meet the requirements put forth in the SOO. |  |
| **Section 7 – Personnel, Qualifications, and Staffing -** Quoters shall clearly identify all key personnel that will be designated as such if an award is made and subject to the applicable key personnel clause, as well as other staff proposed to have major responsibilities, and describe the qualifications of each of the personnel and their corresponding role in achieving the objectives of each task (including labor categories and level of effort). |  |
| **Section 7 – Personnel, Qualifications, and Staffing -** A staffing plan, including an organizational chart, should be included to show lines of authority and responsibility. |  |
| **Section 7 – Personnel, Qualifications, and Staffing -** Qualifications encompass technical knowledge of and experience with, the functions, activities and tasks described in the SOO. |  |
| **Section 7 – Personnel, Qualifications, and Staffing -** Assurances of the commitment of proposed staff must be included. |  |
| **Section 7 – Personnel, Qualifications, and Staffing –** Note that the quoter must submit resumes for all proposed personnel as an appendix to the technical proposal. The resumes must clearly demonstrate the necessary skills, depth of experience, training and professional qualifications to fulfill the roles and responsibilities identified in the prescribed PWS. |  |
| **Appendix 1 – Resumes –** Note that the quoter must submit resumes for all proposed personnel as an appendix to the technical proposal. The resumes must clearly demonstrate the necessary skills, depth of experience, training and professional qualifications to fulfill the roles and responsibilities identified in the prescribed PWS. |  |
| **Appendix 2 – PWS for BPA Task Order –** Quoters must provide a performance work statement (PWS) (Appendix # 2 of the technical quotation) outlining the activities/outcomes that will be accomplished by the quoter in order to satisfy the objectives outlined in the Statement of Objectives (SOO) (See Attachment #2 to solicitation) for the BPA task order. The PWS must use terms/phrases that require/obligate the contractor to fulfill the activities/outcomes. Examples of such terms/phrases include: “the contractor shall complete an analysis to determine …” “The contractor shall deliver a detailed list of…” |  |
| **Appendix 2 – PWS for BPA Task Order – Introduction Section –** This section introduces the parties (FSIS and contractor) |  |
| **Appendix 2 – PWS for BPA Task Order – Background Section-** This section elaborates on the background information surrounding the PHIS design and development requirements such as the objectives of the task order. |  |
| **Appendix 2 – PWS for BPA Task Order – Scope of Work Section-** Similar to an executive summary, this section provides an overview of the tasks to be completed. |  |
| **Appendix 2 – PWS for BPA Task Order – Tasks Section –** This section provides a detailed elaboration of the tasks/activities that will occur. Note that this section does NOT state how the tasks will be completed. The detail of how the tasks will be accomplished is reserved for the Technical Work Plan. |  |
| **Appendix 2 – PWS for BPA Task Order – Delivery Schedule Section –** This section elaborates on the date in which each proposed deliverable/service will be rendered to the Department. |  |
| **Appendix 2 – PWS for BPA Task Order – Performance Standards Section**- This section provides a performance standard in which FSIS will use to judge success/failure of each proposed service/deliverable. |  |
| **Appendix 2 – PWS for BPA Task Order – Assumptions Section** – This section clearly delineates any performance assumptions supporting the proposed tasks. This section should NOT include technical or business/pricing assumptions that are traditionally posed in the business/technical volume. |  |
| **Appendix 2 – PWS for BPA Task Order – Constraints Section** – This section elaborates on the operating constraints in which the quoter expects to perform the tasks. |  |
| **Appendix 2 – PWS for BPA Task Order – Government Furnished Equipment Section –** This section clearly outlines any Government furnished equipment that must be rendered to the contractor in order to enable the completion of the proposed services/deliverables. |  |
| **Appendix 2 – PWS for BPA Task Order – Government Furnished Information Section-** This section clearly outlines any Government furnished Information that must be rendered to the contractor in order to enable the completion of the proposed services/deliverables. |  |
| **Appendix 2 – PWS for BPA Task Order – Place of Performance Section** – This section states the place of performance. It should be noted that, due to certain objectives, the place of performance is expected to be variable |  |
| **Appendix 2 – PWS for BPA Task Order –** Quoters are expected to clearly demonstrate a thoughtful and unique approach for developing and executing task order 1. Proposed personnel must have considerable experience in system design and development. Quoters must propose the most effective methods for carrying out tasks described in the SOO. Quoters shall indicate how they propose to carry out all of the objectives and tasks and not merely repeat the language of the SOO. |  |
| **Appendix 2– PWS for BPA Task Order –** Quoters may find it necessary to adjust the schedule provided in the SOO in accordance with the strategies, operations and procedures that they propose. In such a circumstance, quoters shall clearly identify any changes form the schedule laid out in the SOO and explain the rationale for these changes. Quoters should keep in mind that it is FSIS’s intent that the contractor move forward with all work as quickly as possible while maintaining the high quality of products and services. |  |
| **Appendix 3 – Compliance Matrix –** This matrix should crosswalk requirements with the paragraph and page number in the proposed quotation. |  |
| **Appendix 4 – CMMI Level certification document** |  |
| **Appendix 5 – IT Systems Security Information** |  |
| **Appendix 6 – Signed Rules of Behavior** |  |
| **Appendix 7 – 508 Product Assessment Template** |  |

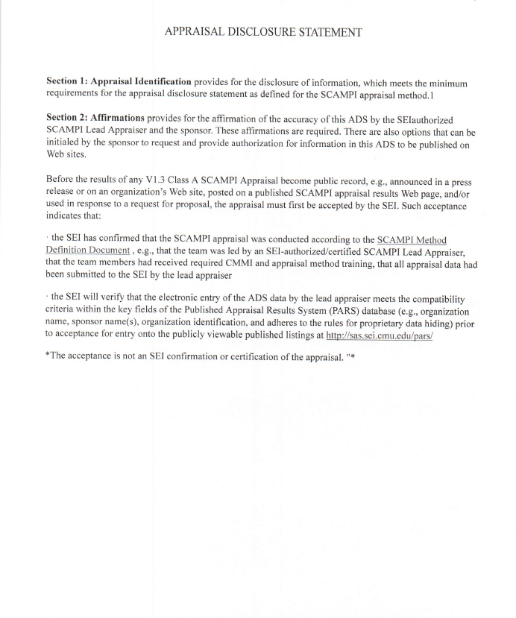
# Appendix 4: CMMI Level 3 Certification

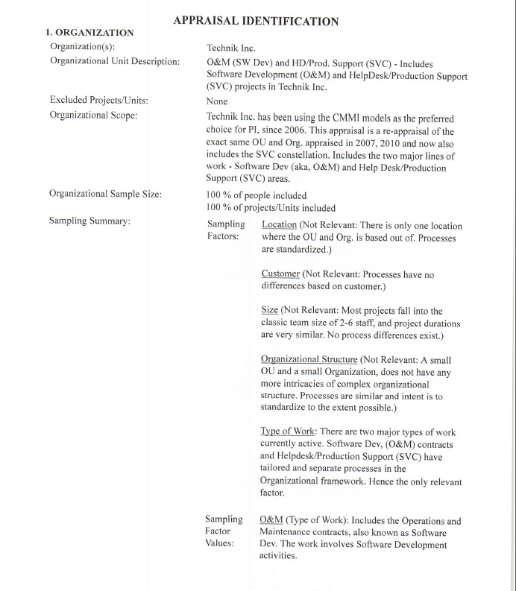
Technik, Inc. has been appraised at Maturity Level 3 on the Capability Maturity Model Integration (CMMI) for Development and Services, v1.3, based on a Standard CMMI Based Appraisal Method for Process Improvement (SCAMPI) Class A, v1.3 Appraisal, completed on September 25, 2012. The appraisal expires on September 25, 2015. Technik is scheduled to be re-appraised September 7 – 11, 2015.

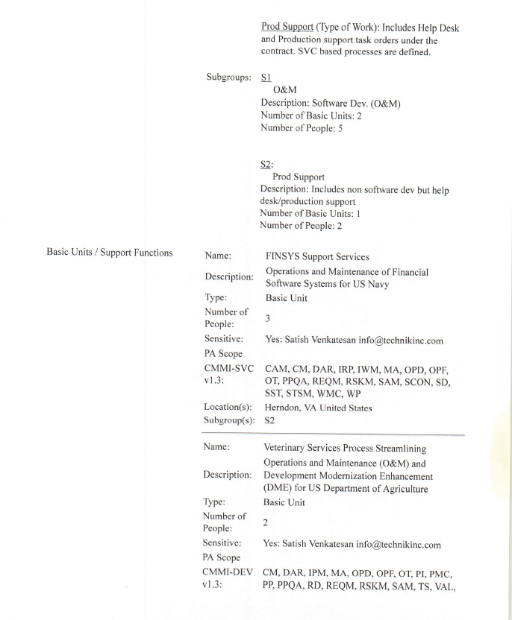
## Technik CMMI Recognition of Achievement

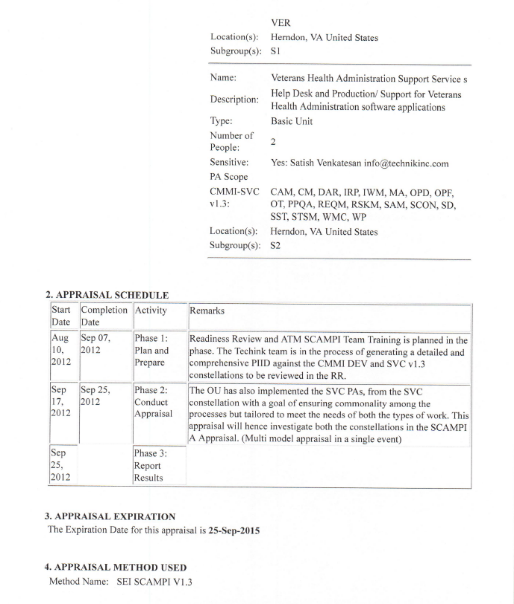


## Technik CMMI Appraisal Disclosure Statement

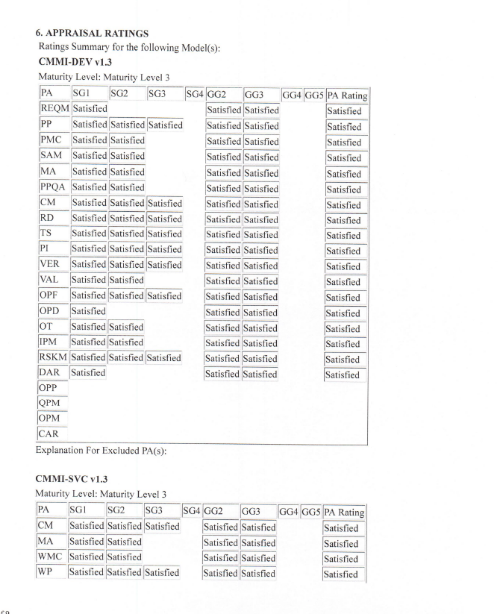


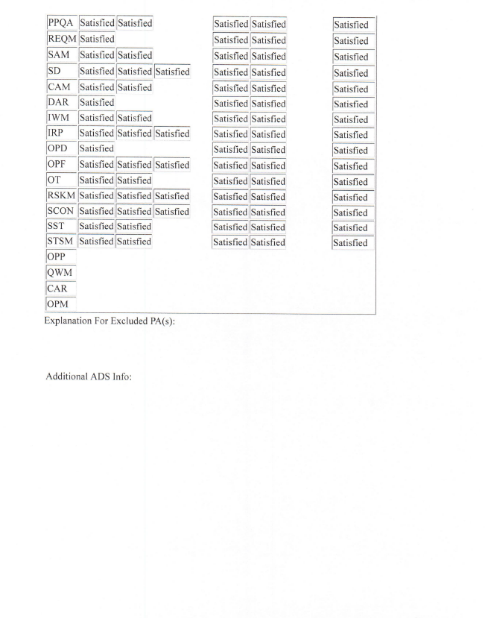


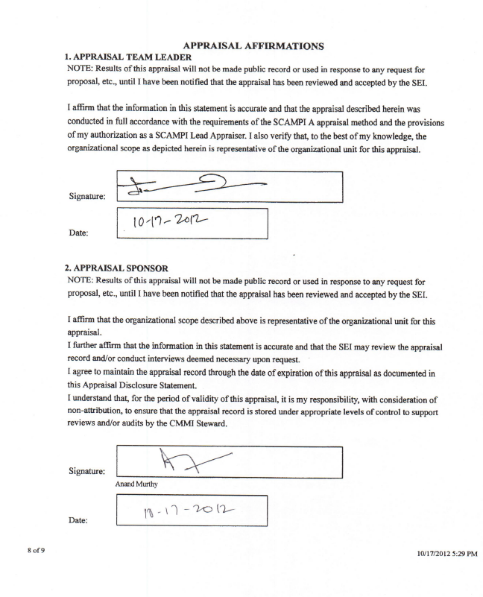












# Appendix 5: Information Technology Systems Security Information

**I.3.5 INFORMATION TECHNOLOGY SYSTEMS SECURITY (SEPT 2013)**

The activities covered under by this contract shall require the Contractor’s access to Federal Automated Information System or systems, as well as the implementation of new systems. The Quoter’s proposal must include:

(1) A detailed outline (commensurate with the size and complexity of the Statement of Work) of its present and proposed information technology systems security program. The response must demonstrate that it complies with the security requirements of the SOW, the Federal Information Security Management Act of 2002 (FISMA, Public Law 107-347, 44 U.S.C. 3531-3536); Office of Management and Budget (OMB) Circular A-130, Appendix III “Security of Federal Automated Information Systems” (http://www.whitehouse.gov/omb/circulars\_a130\_a130appendix\_iii) and an acknowledgement of its understanding of the security requirements of the SOW.

(2) A signed copy of the USDA FSIS IT Rules of Behavior shall be included with the Quoter’s proposal.

Technik has built its Federal security program from applicable laws, regulations and standards. We have developed various organizational policies and programs that ensure compliance with the Federal Information Security Management Act of 2002 (FISMA, Public Law 107-347, 44 U.S.C. 3531-3536); Office of Management and Budget (OMB) Circular A-130, Appendix III “Security of Federal Automated Information Systems”. Technik’s policies and activities are the responsibility of all Technik personnel and not the sole responsibility of one individual. The Information System Security Officer (ISSO) has overall responsibility of an organization’s Information Security Program.

## Security Laws and Regulations

### Federal Information Security Management Act

The Federal Information Security Management Act (FISMA) of 2002, which was passed as TITLE X of The Homeland Security Act (signed into law on November 27, 2002) replaced GISRA and repealed The Computer Security Act Section 11332 of Title 40, United States Code. FISMA provides a framework to ensure the security controls used to protect the federal assets are effective and grants more responsibility to the National Institute of Standards and Technology (NIST) to develop and maintain standards for minimum information security controls. Compliance with the standards is mandatory.

### Office of Management and Budget Circular A-130

Office of Management and Budget (OMB) Circular A-130, Appendix III calls for a management authorization for major applications and general support systems to process information3. That authorization is based on an assessment of the management, operational, and technical controls put in place to protect an organizations information technology resources. The resources assessed include the hardware, software, data, and people that are part of the business processes supporting the organization’s mission(s). The authorization by the management official should occur at least every three years or whenever a major modification of the application or system happens. Other laws and regulations that may be applicable to an organization and may provide requirements for their information security program are identified below..

* U.S. Privacy Act, 1974 (as Amended)
* U.S. Electronic Communications Privacy Act, October 1986
* U.S. Computer Abuse Amendments Act, January 1995
* U.S. Economic and Protection of Proprietary Information Act, October 1996
* U.S. Kennedy-Kassenbaum Health Insurance and Portability Accountability
* Act (HIPAA), October 2002
* U.S. National Information Infrastructure Protection Act, October 1996
* Telecommunications Act of 1996 (Clinger-Cohen Act of 1996)

## Security Standards and Best Practices

### National Institute of Standards and Technology

The National Institute of Standards and Technology (NIST) has developed a library of guidance and standards (http://csrc.nist.gov/publications/) which can be used to help organize an information security program to protect an organization’s information technology assets. The NIST Special Publications (SP), 800 series, established in 1990, provides research and guidance in computer security working with industry, government, and academic organizations. These documents provide approved guidance that the organizations within the federal government are now required to follow4. NIST SP 800-37, *Guidelines for the Security Certification and Accreditation of Federal Information Systems*, provides a methodology for certifying the security of the technology, policies, and procedures that an organization has in place that protects the confidentiality, integrity, and availability of their information assets5. As defined in 44 United States Code (USC), Section 3542, the confidentiality, integrity, and availability of an information asset is:

* Confidentiality – “Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…”
* Integrity - “Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…”
* Availability - “Ensuring timely and reliable access to and use of information…” Other NIST Publications, which provides guidance for developing different areas of an organization’s information security program and support the certification of information systems, are identified below.
* NIST 800-12, An Introduction to Computer Security; The NIST Handbook
* NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems
* NIST SP 800-30, Risk Management Guide for Information Technology Systems
* NIST SP 800-53, DRAFT, Guide to Information Technology Security Services
* NIST FIPS PUB 199, DRAFT, Standards for Security Categorization of Federal Information and Information Systems
* NIST FIPS PUB 102, Guideline for Computer Security Certification and Accreditation

### International Organization for Standardization

The ISO 17799 standard is a detailed security standard that lists ISO identified best practices of the information security arena. The international standard is composed of two parts, ISO 17799 - a method of practice and BS-7799-2 - specifications for an information management system. The standard is organized into ten major sections covering different aspects of information security.

* Business Continuity Planning
* System Access Control
* System Development and Maintenance
* Physical and Environmental Security
* Compliance
* Personnel Security
* Security Organization
* Computer & Network Management
* Asset Classification and Control
* Security Policy

Many organizations accept the ISO 17799 as reputable standards to use for constructing an information security program.

### SANS (SysAdmin, Audit, Network, Security)

SANS is an established institute recognized for its research, education, and certification of individuals in the information security profession. SANS also provides a medium for these professionals to share their lessons learned. This community is made of individuals working in government, educational and civil organizations from around the world. SANS supports many ongoing programs to promote secure computing environments using best practices that have been identified, discussed, and validated by the information security professionals. Security Consensus Operational Readiness Evaluation (SCORE) is an effort between SANS and the Center for Internet Security (CIS) to promote these best practices (http://www.sans.org/score/) and make them available to the security community at large.

### Center for Internet Security

The Center for Internet Security (CIS) is a non-profit organization that provides other organizations methods and tools to improve, measure, monitor, and compare the security status of an organization’s Internet-connected systems and appliances6. The CIS works with a large member group consisting of vendors and individual users that identify security threats that are of concern to the members in the group. Working with the member community, and as stated by the CIS web page, the CIS makes available *Internet security benchmarks* that are “based on recognized best practices for deployment, configuration, and operation of network systems.” The CIS benchmarks are developed in an attempt to cover three factors in Internet-based attacks: technology, processes, and human behavior. All benchmarks are made available to the public and be found at <http://www.cisecurity.org/benchmarks.html>.

### ORGANIZATION’S SUPPORTING PROGRAMS

An organization will normally have a multitude of different policies and programs, Figure 2 – Organization’s Supporting Security Policies & Programs, that may not all be the responsibility of the ISSO. Even so, a large portion of these policies and programs directly or in-directly support an organizations information security program and the certification and accreditation (C&A) of the organization’s information systems. The subjects identified here all play some role in the overall protection of organizations information assets and while this list is not all inclusive, it does help establish an overall security program.

## Technik Security Policies

A comprehensive information security program requires an approach that reaches beyond the areas that most normal information technology people consider. Senior management has overall responsibility for the protection of an organization’s information assets. A comprehensive program begins with a senior management official promulgating an organizational information security policy that establishes, at a high-level, the purpose and scope of the program and defines different organization roles and responsibilities by position. The information security program depends upon the responsibilities and actions of the other offices in performing their responsibilities outlined in the policy which help in the protecting the organizations information assets. Once the information security policy has been established, specific additional policies will establish support for different specific areas that play a role in protecting the organizations information assets. During the C&A process the policies are used as a reference point to validate that the application or general purpose system meets the requirements outlined within these policies. Some topic specific policies that should be considered for development that will play a role in protecting an organization’s information assets include:

* Security Organization
* System and Data Identification (Assets Classification and Control)
* Personnel Security
* Physical Security
* System Access Control
* Computer and Network Management
* Incident Response
* System Development Life Cycle
* System Configuration Management (hardware and software maintenance)
* Business Continuity Planning and Disaster Recovery Planning.

### Physical Security

While information security professionals may take actions to secure the logical portions of an organization’s information assets, if a system’s components are not physically protected from threats, the security professional’s actions are all done in vain. Physical threats can be any event that causes a disruption of services provided by an information system for an organization. Threats may be man-made or natural, accidental or intentional. An organization’s physical security may include security guards, dogs, and cameras to help monitor and control access to the organization’s grounds, building, and designated spaces (i.e. the computer room or data center). Fire and smoke detection and prevention with environmental controls are essential elements that support parts of an organizations physical security. However, even with all these controls in place manual intervention is still required at some point in the physical security realm. Therefore, each of the controls used at an organization should have operating procedures that have been planned, tested, and implemented. Once tested and implemented the operating procedures will guide personnel through required actions during a physical threat.

### Personnel Security

Another aspect of a security program may require controls in place to reduce risks posed by individuals handling the organization’s information that may be sensitive in nature. This sensitivity could be due to information that is proprietary to the organization’s products or processes or there may be personal data requiring protection in accordance with the Privacy Act of 19748. In any case, the organization must know that the individuals are qualified and trustworthy. In order to do meet these and other requirements each sensitive position should be clearly defined. This definition should outline the work to be completed, the position’s responsibilities, and the sensitivity of the position. To determine a person’s trustworthiness for these positions a screening process, sometimes referred to as a background check will be required. A background check may be as simple as calling the local law authorities to check for a police record. On the other hand, the checks may be so extensive it requires investigations into the person’s history for the past 10 or more years. The background check would be based on the sensitivity of the position and how much funding the organization wants to pay for the process. Once a person(s) is hired to hold the job position(s), the organization should ensure that these individuals are trained to stay proficient in their responsibilities.

### System and Data Identification

OMB Circular A-130, Appendix III defines two primary system categories to assist federal agencies in identifying the systems that support their mission9. General support system or system - an interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization (IPSO). Major application - means an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.” Based on the definitions a general support system is easy to identify however, the major application description has ambiguity that may require an organization to further clarify an identification process to indicate which of their systems are major applications. The identification of they system helps determine the impact of a loss or compromise10 if it were to occur. Therefore, each organization should have a formal documented process in place that helps identify which of their systems are major applications. Factors for consideration in the process may include one or more of the following items.

* The importance of the system or information to the organization’s business process or mission.
* Financial harm to the organization if the system or information where compromised.
* Cost of a systems development, maintenance, and replacement.
* Cost of the information’s development, maintenance, and replacement.
* Harm to the organization’s reputation if the system or information where compromised.
* Would there be a loss of life or limb if the system or information where compromised.

The organization’s business managers and system users will conduct each system’s identification process since these individuals have a better understanding of how the loss or compromise of the asset’s confidentiality, integrity, or availability would affect the organization. NIST has recently promulgated a draft document that provides standard security categories to help identify impact to an organization when there is a loss or compromise of an organization’s information assets. Although this publication is in draft form as of October 2003, it is projected for publication prior to 2004.

### Incident Response Program

An incident response program is essential for any organization that has any automated system supporting any facet of their business process11. The program should be chartered through the organizations information security policies and clearly define the goals of the program granting the authority needed to make the decisions and take the actions required when in the best interest of the organization. The policy should be coordinated with the organization’s senior management to ensure the incident response team has approval from the different internal organizations that may be affected by an incident. A well-formulated incident response program will be multifaceted with a specific team of individuals who have the training, the talents, and the equipment to respond to a computer related anomaly in a timely and effective manner. While technical ability is the fore thought for a computer response team, the organizations legal staff and public affairs office should be included within the team in case there are legal implications or public involvement. Prior to any incident, documentation supporting the program should be in place outlining actions for the different phases. As identified in SANS “Computer Security Incident Handling Step By Step” guide there are six phases that an incident response program should have outlined are:

* Preparation
* Identification
* Containment
* Eradication
* Recovery, and
* Follow-up

Any incident is an undesired event for an organization and having a well thought out incident response program provides a layer of protection for an organization providing logical steps to keep the event from escalating out of control.

### System Security Plan

The purpose of the security plan is to provide an overview of the security requirements of the system and describe the controls that are in place or those controls that are planned for meeting the security requirements. The system security plan also delineates responsibilities and expected behavior of all the individuals who access the system. The security plan should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for the system. It should reflect input from the various managers who are responsible for the system. This includes the information owners, the system operators, the system security manager, and the system administrators. Once developed the system security plan plays a key role in providing an overview of the system for the C&A process. At a minimum, the system security plan should cover the subjects outlined below to keep within the NIST standards 13.

* System Identification
* Responsible Organization
* Information Contact(s)
* Assignment of Security Responsibility
* System Operational Status
* General Description/Purpose
* System Environment
* System Interconnection/Information Sharing
* Applicable Laws or Regulations Affecting the System
* General Description of Information Sensitivity
* Management Controls
* Risk Assessment and Management
* Review of Security Controls
* Rules of Behavior
* Planning for Security in the Life Cycle
* Authorize Processing
* Operational Controls
* Personnel Security
* Physical and Environmental Protection
* Production, Input/Output Controls
* Contingency Planning
* Application Software Maintenance Controls
* Data Integrity/Validation Controls
* Documentation
* Security Awareness and Training
* Incident response capability
* Technical Controls
* Identification and Authentication
* Logical Access Controls
* Public Access Controls
* Audit Trails

The system owner is responsible for maintaining the security plan. Any time there are changes to the system, the security plan should be reviewed and updated as applicable. At a minimum, this should be done on an annual basis. The organizations information security personnel should ensure that the system owners stick to the review and update process since this document should be the first item they review when a system is being assessed in the C&A process.

### System Development Life Cycle

The System Development Life Cycle (SDLC) is a traditional process using a set of logical systematic activities, also known as phases, to develop, implement, and operate a system. Each of the phases have specific activities that integrates the implementation of security into the life cycle process of a system that will make the security controls more effective and potentially reduce the cost of security for the system. NIST identifies five common phases14 in the SDLC process that have some security related actions.

* Initiation Phase
* Acquisition/Development Phase
* Implementation Phase
* Operation/Maintenance Phase
* Disposition Phase

### Configuration Management

Configuration management involves the identification of a system’s configuration at given points in time, systematically controlling changes to the configuration, and maintaining the integrity and traceability of the system configuration throughout the systems lifecycle. The items that should be placed under a configuration management program include the software and hardware products that comprise the system as well as items required to create or maintain these products. A configuration management program should address the following items:

* Identify the proper process for making system changes
* Identify the individuals and organization that made changes to the system
* Identify the changes that were made to the system
* Document when the changes were made to the system
* Document the justification of the changes made to the system
* Document who requested and authorized the system changes

The CM process includes procedures, hardware associated with or supporting the system, software applications, and all network physical and logical configurations and documentation affecting the system. The processes will serve to reduce the discrepancy between what is authorized and what is implemented. The CM process will ensure that the operational system is implementing the correct security policy as promulgated by the organizations security requirements.

### Training and Awareness Program

OMB and FISMA require that each federal organization establish a training program where all personnel within an organization are thoroughly trained in their security responsibilities. An information security-training program accomplishes this for the organization. This program should be established through the organization’s information security policy. This lets all personnel know that the organization’s senior management feels security is important and that everyone will be held accountable for their actions. The training program is the process through which the organization informs the users of the organization’s security policies and practices, what is expected of the users, and how the users are to handle the organization’s information, data, and systems. The training program should provide the relevant and needed security skills and competency to enable the organization’s employees, contractors, and partners to perform their jobs more effectively. Learning methods or activities should concentrate on a particular topic; those topics should be rotated to prevent a particular topic from becoming stale and unnoticed. Topics are not limited and change as technology advances. Some of the NIST recommended topics include, but are not limited to the following items: Password usage and management – including creation, frequency of changes, and protection.

* Protection from viruses, worms, Trojan horses, and other malicious code – scanning, updating definitions
* Policy – implications of noncompliance
* Unknown e-mail/attachments
* Web usage – allowed versus prohibited; monitoring of user activity
* Spam
* Data backup and storage – centralized or decentralized approach
* Social engineering
* Incident response – contact whom? “What do I do?”
* Shoulder surfing
* Changes in system environment – increases in risks to systems and data (e.g., water, fire, dust or dirt, physical access)
* Inventory and property transfer – identify responsible organization and user responsibilities (e.g., media sanitization)
* Personal use and gain issues – systems at work and home
* Handheld device security issues – address both physical and wireless security issues
* Use of encryption and the transmission of sensitive/confidential information over the Internet – address agency policy, procedures, and technical contact for assistance
* Laptop security while on travel – address both physical and information security issues
* Personally owned systems and software at work – state whether allowed or not (e.g., copyrights)
* Timely application of system patches – part of configuration management
* Software license restriction issues – address when copies are allowed and not allowed
* Supported/allowed software on organization systems – part of configuration management
* Access control issues – address least privilege and separation of duties
* Individual accountability – explain what this means in the organization
* Use of acknowledgement statements – passwords, access to systems and data, personal use and gain

An organization’s information security training is one of the most important aspects of computer and information security, building on awareness. An effective training and awareness program reduces the number of accidental security incidents because people are more conscious of general security issues.

### System Documentation

As a part of any organizations well defined SDLC process, the development of documentation specific to the system should be outlined. The documentation would outline the system from development to it’s production state. The documentation may include items identified below.

* System functional requirements,
* Database software configurations,
* Data dictionary,
* Operating system configurations,
* User application configuration,
* System architecture (physical),
* Data flow (logical),
* System interconnections,
* User manuals,
* System security plan,
* disaster recovery/business continuity plan,
* Security test plan,
* Certification statement, and any service level agreements, memorandums of understanding, or memorandums of agreement that was required for the system.

The documentation will support the organizations information security program through its availability allowing authorized and qualified individuals the ability to understand the system configurations and operational state. This assists problem isolation reducing system downtime and provides a baseline for the development of enhancements for the system in the future. Having the right documentation available keeps an organization from depending on the individual(s) who developed the system. The system owner is the party responsible to ensure that the documentation is developed, maintained, and made available to the appropriate people.

### Disaster Recovery

Disaster recovery consists of two areas, a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP). The two areas are established to ensure that an organization’s critical business processes are maintained to support the organization’s primary mission. The BCP provides a strategy to minimize the after effects of a disruptive event while the DRP consist of the actions that must be taken before, during and after a disruption for each system supporting a business process to minimize the losses to the organization. While the goals and actions in these plans are extremely important, the people carrying out these activities are the most critical elements. The plans must ensure that the organization’s personnel are the most important asset and that loss of life or limb outweighs any loss of information or physical asset owned by the organization. Once these plans have been completed, it is extremely important that these plans be proven through testing. Therefore, every plan needs to be tested! The results of the testing will provide lessons learned that would be used to strengthen the plans correcting weaknesses or oversights.

## CERTIFICATION AND ACCREDITATION (C&A) PROGRAM

The C&A of an information system is the process where an independent party verifies that a system meets or exceeds the security requirements identified for protecting an organization’s information system and data. The method used for verification is usually similar no matter who completes the process and consist of five basic steps: identify assets, identify threats and vulnerabilities, collect data (test, inspect, and interview), analyze the data and document the results. Once the results are documented a senior management official reviews and approves, or disapproves the operation of the system based on the results of the verification process.

### Certification Process

The certification process, Figure 3 – An Information System’s Certification Process, consist of activities using established techniques that verify that the system’s security controls as documented in the system’s security plan have been implemented and are effective in mitigating risks to the system. The process takes into consideration a system's operating environment and should identify the other compensating controls in place to protect the system. Another outcome of this process is the identification of vulnerabilities within the system and recommendations to correct the vulnerability. One of the first things to accomplish should be a “kick-off” meeting. This meeting is to get the system support personnel and the security personnel, or certification team, together for an introductory of all personnel involved. The primary objective of this meeting is for the certification team to review the process with the system owner, system security officer, system technical point of contact, and system administrator(s). The meeting provides a forum for all personnel to meet each other discuss the process and make known the rules of engagement for the activities and the materials (documentation) needed for the review and validation processes.

Asset & Threat Identification. The system’s security plan should be reviewed for a description of the system, its security controls, its physical and logical interconnectivity, and the operational environment the system operates within. Threats to the system may also be listed in the system’s security plan however, if they are not, they should be identified at this point in the process. A walk through should be conducted to visually identify the system’s physical components being certified and how the components are interconnected. At this point, the scope of the system’s certification begins to formulate. The scope is to include clear identification of boundaries for testing and any test information that can be reused for other systems at the organization. The certification team may want to meet with the system owner and other applicable personnel to inform them of assets that have been identified, and the scope of the certification process. Familiarization with the assets and their environment will help the certification team determine how the system will be certified and what testing will be conducted for the certification process. A system certification may reuse data from another certification or supply data for other system certifications. This data reuse is accomplished in one of two different situations. One situation would be when you are deploying a specific type of system where the security controls are specific to that system and are not changed no matter where the system is installed. This data is system specific and referred to as type-specific data. The other situation is where you have multiple systems at one location, or site, and you have security controls specific to that site and are applicable for all systems at that one location. This data would be site-specific data. The Department of Defense has used this process during the certification of many of their information systems which saving time and expenses. NIST has also identified this as a viable means to reuse evaluation data that may be applicable to several systems.

A security test and evaluation (ST&E) plan sometimes referred to as a test plan, can then be defined for the certification team’s activities. A very simplistic test plan may look something like Table VII-1, Sample Test Plan, shown on the next page. The test plan can be used as a guide for validating the implementation of the systems security controls that are in place. The control areas to be tested are those security controls described in the system’s security plan: the Management, Operational, and Technical Controls. Each control area has several sub-areas that are more specific and should be tested during the certification process. The plan could identify the method used to test each specific control area being reviewed. Test methods include visual inspections, personnel interviews, documentation review, and use of automated tools that are applicable. The test could also include the potential tool(s) required to conduct the testing and the personnel involved.

**Control Test Method Tool Personnel**

Insert table

**Data Analysis**. Once the data has been collected it must then be organized and analyzed based on the requirements and considering the known existing threats to the system. The analysis should help determine:

* That the security control meets requirements
* If the security control is implemented as documented
* If the security control is appropriate to protect the system and data
* Any known vulnerabilities
* What, if any, corrective actions can be taken to correct or reduce the risk which a vulnerability allows
* What other controls are in place to help mitigate risks to the system

Once the analysis is completed and the potential risk levels have been identified for each vulnerability the certification team should meet with the system owner and the applicable personnel to validate the findings and eliminate any false positives or negatives. During this process negotiations regarding the vulnerabilities risk levels may occur, along with the system owner taking actions to correct vulnerabilities. Either way, these actions may change the vulnerabilities that were originally identified during the certification process therefore changing the overall risk level of the system. All vulnerabilities, corrected and outstanding should be documented to maintain a system history of the systems configuration changes through out its life cycle. This documentation also feeds the certification report used in the accreditation of the system.

**Certification & Accreditation Package** – The output of the certification process is the C&A package document. The C&A package documents the results from the security testing and evaluation and provides the authorizing official with the information needed to make a decision based on the risk level of the system as to whether the system should be authorized for operation. The package must include the results of the testing, an accreditation letter, the system’s security plan, and a plan of actions and milestones for corrective actions (Fix-It Plan). A package, which includes the items listed below, should provide all the appropriate information for the DAA to make an accreditation decision.

**Executive Summary** – This document is from the certifying authority and addressed to the designated approving authority (DAA) summarizing the results of the certification process, outlining the level of risk of the system, identifying any outstanding actions that are required and provides the certifier’s certification recommendation.

**DAA Brief** – This document is the formal presentation used to present the executive summary and describes, at a high level the results of the system certification process.

Accreditation Letter – This document is the official letter to the system owner from the DAA and is the DAA’s formal accreditation statement that informs the system owner of their responsibilities in maintaining the accreditation of the system.

**Risk Acceptance Letter** – This document is an agreement between the system owner and the certifier. The letter documents the level of risk that has been identified for the system. The letter will outline the system owner’s responsibility to ensure that the system’s security posture is maintained in its current environment. It also tells the system owner that any changes to the system should be reviewed by the computer security office for potential vulnerabilities that may change the system’s level of risk.

**Risk Assessment Report** – This document should describe the system’s risk level based on the security controls that are in place to mitigate any vulnerability that have been identified and associated to threats for the system.

**Security Test & Evaluation Results** – The ST&E results are the documented out put from the various steps completed in the ST&E work plan.

**Risk Definitions** – This document identifies the systems threats and associated risks. Risk calculation methodology can also be defined herein.

**Fix-It Plan** – This document summarizes all the identified vulnerabilities and can be potentially used as a work plan for corrective actions. This document, if formatted appropriately, can be used to track the status of any vulnerability and whether it has been accepted and will be mitigated, transferred or ignored.

**System Diagram** – This document identifies the systems architecture at the time it was subjected to the certification process. The diagram can identify any logical and physical connections and indicate the boundaries that were determined for the scope of the certification activities.

**Acronyms** – This document can be included as an appendix to the main report and list any applicable acronyms that are used through out.

**References** – This document can be included as an appendix to the main report and list any references that are applicable to the report or the processes involved.

**System Security Plan** – This document should be a copy of the system’s security plan that describes the system and the security controls that are in place to protect the system.

### Accreditation Process

The certification process provides the documentation of identified vulnerabilities that the certification team and the system owner have reviewed, corrected, and negotiated. Results are documented in the C&A package and undergo an accreditation process such as that indicated in Figure 4, An Information System’s Accreditation Process. The C&A package should be provided to the ISSO for review allowing feedback and approval of the certification teams output from the certification process. The system owner would then be briefed on the C&A package as completed, to include any recommendations or changes that may have been made during the ISSO’s review. Prior to the certifying officer issuing a certification statement, the system owner and certifying officer should be in agreement on the system’s overall level of risk, pending corrective actions and each parities responsibility in completing these actions. The agreement of the system’s risk level and plan to reduce or eliminate any remaining risk to the system by all responsible parties should help the decision process confronting the designated approving authority.

With the C&A package previously outlined, there should be enough information for the DAA to make a decision for the operation of the system. The DAA’s decision is risk-based, and done with the knowledge that the system may have remaining vulnerabilities that pose residual risk to the organization’s remaining assets and operations. After the DAA reviews the C&A package, the system can be accepted or rejected due to the residual risk that the system poses. If rejected, the DAA’s concerns should be corrected if possible. The system will then be re-evaluated to verify that controls have been put in place to eliminate or reduce the risk that was previously identified. If accepted an accreditation statement is issued for the system. There are two types of accreditations that may be issued for a system: 1) approval to operate (ATO) or 2) intermediate approval to operate (IATO). The ATO indicates that the system has been approved for period of time, typically a period of three years19 or when significant changes are made to the system’s architecture. The IATO indicates that a system has a limited approval for a specific period of time that is determined by the approving authority and may be based on the risk level of the system. For a system with an IATO, the goal is controls are put in place for vulnerabilities identified so that at the end of the specified period the system can be accredited with an ATO.

### Post Accreditation Activities

Several post activities should be accomplished after the accreditation of an information system, Figure 5 – Post Accreditation Activities. During the C&A process documentation should have a proposed “Fix- it Plan” developed as a part of the C&A package. After the system has been accredited, the fix-it plan can be used as a management tool for tracking corrective actions that need to be completed to correct the vulnerabilities identified during the system’s C&A process. The system should also be subject to applicable patches and updates that become available for the operating system, middleware and any other applications or components of the system. The patches and updates should be tested in a development environment prior to implementing in the production environment. This testing will help determine what changes could be made to the system when the patch or update is installed to make sure no other vulnerabilities are introduced to the system. This testing scenario should also include planned changes or controls that had not yet been implemented. The accredited systems should also be scheduled for scans conducted no less than annually to ensure that the integrity of the system’s technical security posture has not changed from what was identified during the certification process. Additionally, the organization should consider implementing an active monitoring program to alert appropriate personnel (i.e. technical or security staff) of any unauthorized or undesired activities that may be occurring to the organization’s systems. All of these post accreditation activities help identify and mitigate risks to an organizations information systems. All activities can provide lessons learned which could be used to support new organizational policies, policy changes, and program development and implementation. The same lessons learned can also provide input into the certification process for future systems or re-accreditation processes.

## SUMMARY

Some of the areas supporting the information security program may be required by law or regulations where others may be considered a best practice. To help meet these requirements the information security policy could be promulgated from an organization’s senior executive. This informs management that the organization takes information security seriously. The policy could identify the other department’s responsibilities, through their policies or programs, in the protection of the organizations information assets. The verification that these policies and programs are being implemented effectively an organization means having the information systems subjected to the C&A review process. The C&A process can provide the organization feedback on how well they are meeting or exceeding regulatory or organizational requirements. NIST has published a small library providing guidance that an organization can use in the development of their information security program. While these documents are not required by the commercial sector, they can still be used to establish a sound program.

# Appendix 6: Signed Rules of Behavior Document

**Food Safety and Inspection Service (FSIS)**

**Information Technology (IT) Security**

**Rules of Behavior for Privileged Users**

**Version 1.0**

**February 10, 2006**

**INTRODUCTION**

**PURPOSE**

The intent of the FSIS Rules of Behavior (ROB) for Privileged Users is to recognize the additional responsibilities associated with special access to, and/or privileges associated with, computer resources within the Department or its offices/bureaus/components. The ROB for Privileged Users are in addition to the Computer System User IT Security General ROB to which all DOJ users are subject. The identification of these responsibilities originates in OMB A-130 and is included in the FSIS IT Security Standards.

*“Privileged User” defined:*

A privileged user is someone authorized access to departmental/office/bureau/component computer resources when that access provides the capability to alter the properties, behavior or control of the information system/network. It includes, but is not limited to, any of the following types of access:

1. “Super user,” “root,” or equivalent access, such as access to the control functions of the information system/network, administration of user accounts, etc.
2. Access to change control parameters (e.g., routing tables, path priorities, addresses) of routers, multiplexers, and other key information system/network equipment or software.
3. Ability and authority to control and change program files, and other users’ access to data.
4. Direct access to operating system level functions (also called unmediated access) that would permit system controls to be bypassed or changed.
5. Access and authority for installing, configuring, monitoring or troubleshooting the security monitoring functions of information systems/networks (e.g., network/system analyzers; intrusion detection software; firewalls) or in performance of cyber/network operations.

*Who is covered by these rules?*

These rules extend to all privileged users (FSIS employees and contractors) who use any computing resources that support the mission and functions of the Food Safety and Inspection Service. All privileged users will review and provide signature or electronic verification to these rules annually, or upon change of assigned responsibilities, whichever occurs first.

*What are the penalties for Noncompliance?*

Compliance with these rules will be enforced through sanctions commensurate with the level of infraction. Actions may include a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, or termination, depending on the severity of the violation. In addition, activities that lead to or cause the disclosure of classified information may result in criminal prosecution under the U.S. Code, Title 18, Section 798, and other applicable statutes.

**RESPONSIBILITIES**

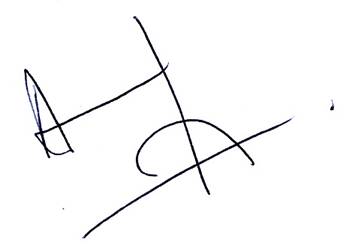
*Complying Privileged Users will:*

1. Understand that it is their responsibility to comply with all security measures necessary to prevent the unauthorized disclosure, modification, or destruction of information; follow appropriate system security policies, guidelines and procedures
2. Agree to the FSIS General Rules of Behavior.
3. Minimize exposure and risk by utilizing a separate account to perform privileged functions from general user functions.
4. Not establish or reset any account utilizing the same password for more than one account, and will not provide the user name and password at the same time through the same medium.
5. Grant read or write authority no higher than is granted to him/her (e.g., a component level user administrator shall not assign department level access to another user administrator).
6. Access application programs only for the purpose of creating or maintaining files.
7. Not make modifications to system configurations that could impact availability or security of the system without the approval of the Change Control Board and/or change management process.
8. Not perform general user activities under the same account (user name and password) due to the security requirement for separation of duties.
9. Protect all passwords from unauthorized disclosure.
10. Not share accounts with another privileged user.
11. Make the system available at any time to the SAISO for inspection and review of audit logs.
12. Grant only read-only access to audit files to the Security Auditor; grant access to general system information only if a need-to-know is established and authorization is received from the ISSO.
13. Make the computer(s) available for periodic reviews of the security configuration by independent testers
14. Make changes to system configuration as directed to meet Vulnerability and Patch Management requirements.
15. Immediately record and report any security incidents to the ISSPM.

I acknowledge and understand the responsibilities associated with my role as a Privileged User, and I will comply with the February 10, 2006, Privileged User Rules of Behavior. *The Statement of acknowledgement can be provided via email.*

Anand Murthy

Typed Name



\_\_\_\_\_\_\_\_ \_ 8/27/2015

Signature Date

[End of Document]

# Appendix 7: Section 508 Product Assessment Template

The contractor shall provide a completed Section 508 Product Assessment Template and the contractor shall state exactly how proposed Electronic and Information Technology (EIT) deliverable(s) meet or does not meet the applicable standards.

|  |  |  |
| --- | --- | --- |
| **Summary Table** | | |
| **Criteria** | **Supporting Features** | **Remarks and Explanations** |
| Section 1194.21 Software Applications and Operating Systems |  |  |
| Section 1194.22 Web-based internet information and applications |  |  |
| Section 1194.23 Telecommunications Products |  |  |
| Section 1194.24 Video and Multi-media Products |  |  |
| Section 1194.25Self-Contained, Closed Products |  |  |
| Section 1194.26 Desktop and Portable Computers |  |  |
| \*\* Section 1194.31 Functional Performance Criteria |  |  |
| \*\* Section 1194.41 Information, documentation, and support. |  |  |

|  |  |  |
| --- | --- | --- |
| **Section 1194.21 Software Applications and Operating Systems** | | |
| **Criteria** | **Supporting Features** | **Remarks and Explanations** |
| (a) When software is designed to run on a system that has a keyboard, product functions shall be executable from a keyboard where the function itself or the result of performing a function can be discerned textually. |  |  |
| (b) Applications shall not disrupt or disable activated features of other products that are identified as accessibility features, where those features are developed and documented according to industry standards. Applications also shall not disrupt or disable activated features of any operating system that are identified as accessibility features where the application programming interface for those accessibility features has been documented by the manufacturer of the operating system and is available to the product developer. |  |  |
| (c) A well-defined on-screen indication of the current focus shall be provided that moves among interactive interface elements as the input focus changes. The focus shall be programmatically exposed so that Assistive Technology can track focus and focus changes. |  |  |
| (d) Sufficient information about a user interface element including the identity, operation and state of the element shall be available to Assistive Technology. When an image represents a program element, the information conveyed by the image must also be available in text. |  |  |
| (e) When bitmap images are used to identify controls, status indicators, or other programmatic elements, the meaning assigned to those images shall be consistent throughout an application's performance. |  |  |
| (f) Textual information shall be provided through operating system functions for displaying text. The minimum information that shall be made available is text content, text input caret location, and text attributes. |  |  |
| (g) Applications shall not override user selected contrast and color selections and other individual display attributes. |  |  |
| (h) When animation is displayed, the information shall be displayable in at least one non-animated presentation mode at the option of the user. |  |  |
| (i) Color coding shall not be used as the only means of conveying information, indicating an action, prompting a response, or distinguishing a visual element. |  |  |
| (j) When a product permits a user to adjust color and contrast settings, a variety of color selections capable of producing a range of contrast levels shall be provided. |  |  |
| (k) Software shall not use flashing or blinking text, objects, or other elements having a flash or blink frequency greater than 2 Hz and lower than 55 Hz. |  |  |
| (l) When electronic forms are used, the form shall allow people using Assistive Technology to access the information, field elements, and functionality required for completion and submission of the form, including all directions and cues. |  |  |

|  |  |  |
| --- | --- | --- |
| **Section 1194.22 Web-based Internet information and applications** | | |
| **Criteria** | **Supporting Features** | **Remarks and Explanations** |
| (a) A text equivalent for every non-text element shall be provided (e.g., via "alt", "longdesc", or in element content). |  |  |
| (b) Equivalent alternatives for any multimedia presentation shall be synchronized with the presentation. |  |  |
| (c) Web pages shall be designed so that all information conveyed with color is also available without color, for example from context or markup. |  |  |
| (d) Documents shall be organized so they are readable without requiring an associated style sheet. |  |  |
| (e) Redundant text links shall be provided for each active region of a server-side image map. |  |  |
| (f) Client-side image maps shall be provided instead of server-side image maps except where the regions cannot be defined with an available geometric shape. |  |  |
| (g) Row and column headers shall be identified for data tables. |  |  |
| (h) Markup shall be used to associate data cells and header cells for data tables that have two or more logical levels of row or column headers. |  |  |
| (i) Frames shall be titled with text that facilitates frame identification and navigation |  |  |
| (j) Pages shall be designed to avoid causing the screen to flicker with a frequency greater than 2 Hz and lower than 55 Hz. |  |  |
| (k) A text-only page, with equivalent information or functionality, shall be provided to make a web site comply with the provisions of this part, when compliance cannot be accomplished in any other way. The content of the text-only page shall be updated whenever the primary page changes. |  |  |
| (l) When pages utilize scripting languages to display content, or to create interface elements, the information provided by the script shall be identified with functional text that can be read by Assistive Technology. |  |  |
| (m) When a web page requires that an applet, plug-in or other application be present on the client system to interpret page content, the page must provide a link to a plug-in or applet that complies with 1194.21(a) through (l). |  |  |
| (n) When electronic forms are designed to be completed on-line, the form shall allow people using Assistive Technology to access the information, field elements, and functionality required for completion and submission of the form, including all directions and cues. |  |  |
| (o) A method shall be provided that permits users to skip repetitive navigation links. |  |  |
| (p) When a timed response is required, the user shall be alerted and given sufficient time to indicate more time is required. |  |  |

Note to 1194.22: The Board interprets paragraphs (a) through (k) of this section as consistent with the following priority 1 Checkpoints of the Web Content Accessibility Guidelines 1.0 (WCAG 1.0) (May 5 1999) published by the Web Accessibility Initiative of the World Wide Web Consortium: Paragraph (a) - 1.1, (b) - 1.4, (c) - 2.1, (d) - 6.1, (e) - 1.2, (f) - 9.1, (g) - 5.1, (h) - 5.2, (i) - 12.1, (j) - 7.1, (k) - 11.4.

|  |  |  |
| --- | --- | --- |
| **Section 1194.23 Telecommunications Products** | | |
| **Criteria** | **Supporting Features** | **Remarks and Explanations** |
| (a) Telecommunications products or systems which provide a function allowing voice communication and which do not themselves provide a TTY functionality shall provide a standard non-acoustic connection point for TTYs. Microphones shall be capable of being turned on and off to allow the user to intermix speech with TTY use. |  |  |
| (b) Telecommunications products which include voice communication functionality shall support all commonly used cross-manufacturer non-proprietary standard TTY signal protocols. |  |  |
| (c) Voice mail, auto-attendant, and interactive voice response telecommunications systems shall be usable by TTY users with their TTYs. |  |  |
| (d) Voice mail, messaging, auto-attendant, and interactive voice response telecommunications systems that require a response from a user within a time interval, shall give an alert when the time interval is about to run out, and shall provide sufficient time for the user to indicate more time is required. |  |  |
| (e) Where provided, caller identification and similar telecommunications functions shall also be available for users of TTYs, and for users who cannot see displays. |  |  |
| (f) For transmitted voice signals, telecommunications products shall provide a gain adjustable up to a minimum of 20 dB. For incremental volume control, at least one intermediate step of 12 dB of gain shall be provided. |  |  |
| (g) If the telecommunications product allows a user to adjust the receive volume, a function shall be provided to automatically reset the volume to the default level after every use. |  |  |
| (h) Where a telecommunications product delivers output by an audio transducer which is normally held up to the ear, a means for effective magnetic wireless coupling to hearing technologies shall be provided. |  |  |
| (i) Interference to hearing technologies (including hearing aids, cochlear implants, and assistive listening devices) shall be reduced to the lowest possible level that allows a user of hearing technologies to utilize the telecommunications product. |  |  |
| (j) Products that transmit or conduct information or communication, shall pass through cross-manufacturer, non-proprietary, industry-standard codes, translation protocols, formats or other information necessary to provide the information or communication in a usable format. Technologies which use encoding, signal compression, format transformation, or similar techniques shall not remove information needed for access or shall restore it upon delivery. |  |  |
| (k)(1) Products which have mechanically operated controls or keys shall comply with the following: Controls and Keys shall be tactilely discernible without activating the controls or keys. |  |  |
| (k)(2) Products which have mechanically operated controls or keys shall comply with the following: Controls and Keys shall be operable with one hand and shall not require tight grasping, pinching, twisting of the wrist. The force required to activate controls and keys shall be 5 lbs. (22.2N) maximum. |  |  |
| (k)(3) Products which have mechanically operated controls or keys shall comply with the following: If key repeat is supported, the delay before repeat shall be adjustable to at least 2 seconds. Key repeat rate shall be adjustable to 2 seconds per character. |  |  |
| (k)(4) Products which have mechanically operated controls or keys shall comply with the following: The status of all locking or toggle controls or keys shall be visually discernible, and discernible either through touch or sound. |  |  |

|  |  |  |
| --- | --- | --- |
| **Section 1194.24 Video and Multi-media Products** | | |
| **Criteria** | **Supporting Features** | **Remarks and Explanations** |
| (a) All analog television displays 13 inches and larger, and computer equipment that includes analog television receiver or display circuitry, shall be equipped with caption decoder circuitry which appropriately receives, decodes, and displays closed captions from broadcast, cable, videotape, and DVD signals. As soon as practicable, but not later than July 1, 2002, widescreen digital television (DTV) displays measuring at least 7.8 inches vertically, DTV sets with conventional displays measuring at least 13 inches vertically, and stand-alone DTV tuners, whether or not they are marketed with display screens, and computer equipment that includes DTV receiver or display circuitry, shall be equipped with caption decoder circuitry which appropriately receives, decodes, and displays closed captions from broadcast, cable, videotape, and DVD signals. |  |  |
| (b) Television tuners, including tuner cards for use in computers, shall be equipped with secondary audio program playback circuitry. |  |  |
| (c) All training and informational video and multimedia productions which support the agency's mission, regardless of format, that contain speech or other audio information necessary for the comprehension of the content, shall be open or closed captioned. |  |  |
| (d) All training and informational video and multimedia productions which support the agency's mission, regardless of format, that contain visual information necessary for the comprehension of the content, shall be audio described. |  |  |
| (e) Display or presentation of alternate text presentation or audio descriptions shall be user-selectable unless permanent. |  |  |

|  |  |  |
| --- | --- | --- |
| **Section 1194.25 Self-Contained, Closed Products** | | |
| **Criteria** | **Supporting Features** | **Remarks and Explanations** |
| (a) Self contained products shall be usable by people with disabilities without requiring an end-user to attach Assistive Technology to the product. Personal headsets for private listening are not Assistive Technology. |  |  |
| (b) When a timed response is required, the user shall be alerted and given sufficient time to indicate more time is required. |  |  |
| (c) Where a product utilizes touchscreens or contact-sensitive controls, an input method shall be provided that complies with §1194.23 (k) (1) through (4). |  |  |
| (d) When biometric forms of user identification or control are used, an alternative form of identification or activation, which does not require the user to possess particular biological characteristics, shall also be provided. |  |  |
| (e) When products provide auditory output, the audio signal shall be provided at a standard signal level through an industry standard connector that will allow for private listening. The product must provide the ability to interrupt, pause, and restart the audio at anytime. |  |  |
| (f) When products deliver voice output in a public area, incremental volume control shall be provided with output amplification up to a level of at least 65 dB. Where the ambient noise level of the environment is above 45 dB, a volume gain of at least 20 dB above the ambient level shall be user selectable. A function shall be provided to automatically reset the volume to the default level after every use. |  |  |
| (g) Color coding shall not be used as the only means of conveying information, indicating an action, prompting a response, or distinguishing a visual element. |  |  |
| (h) When a product permits a user to adjust color and contrast settings, a range of color selections capable of producing a variety of contrast levels shall be provided. |  |  |
| (i) Products shall be designed to avoid causing the screen to flicker with a frequency greater than 2 Hz and lower than 55 Hz. |  |  |
| (j) (1) Products which are freestanding, non-portable, and intended to be used in one location and which have operable controls shall comply with the following: The position of any operable control shall be determined with respect to a vertical plane, which is 48 inches in length, centered on the operable control, and at the maximum protrusion of the product within the 48 inch length on products which are freestanding, non-portable, and intended to be used in one location and which have operable controls. |  |  |
| (j)(2) Products which are freestanding, non-portable, and intended to be used in one location and which have operable controls shall comply with the following: Where any operable control is 10 inches or less behind the reference plane, the height shall be 54 inches maximum and 15 inches minimum above the floor. |  |  |
| (j)(3) Products which are freestanding, non-portable, and intended to be used in one location and which have operable controls shall comply with the following: Where any operable control is more than 10 inches and not more than 24 inches behind the reference plane, the height shall be 46 inches maximum and 15 inches minimum above the floor. |  |  |
| (j)(4) Products which are freestanding, non-portable, and intended to be used in one location and which have operable controls shall comply with the following: Operable controls shall not be more than 24 inches behind the reference plane. |  |  |

|  |  |  |
| --- | --- | --- |
| **Section 1194.26 Desktop and Portable Computers** | | |
| **Criteria** | **Supporting Features** | **Remarks and Explanations** |
| (a) All mechanically operated controls and keys shall comply with §1194.23 (k) (1) through (4). |  |  |
| (b) If a product utilizes touchscreens or touch-operated controls, an input method shall be provided that complies with §1194.23 (k) (1) through (4). |  |  |
| (c) When biometric forms of user identification or control are used, an alternative form of identification or activation, which does not require the user to possess particular biological characteristics, shall also be provided. |  |  |
| (d) Where provided, at least one of each type of expansion slots, ports and connectors shall comply with publicly available industry standards |  |  |

|  |  |  |
| --- | --- | --- |
| **Section 1194.31 Functional Performance Criteria** | | |
| **Criteria** | **Supporting Features** | **Remarks and Explanations** |
| (a) At least one mode of operation and information retrieval that does not require user vision shall be provided, or support for Assistive Technology used by people who are blind or visually impaired shall be provided. |  |  |
| (b) At least one mode of operation and information retrieval that does not require visual acuity greater than 20/70 shall be provided in audio and enlarged print output working together or independently, or support for Assistive Technology used by people who are visually impaired shall be provided. |  |  |
| (c) At least one mode of operation and information retrieval that does not require user hearing shall be provided, or support for Assistive Technology used by people who are deaf or hard of hearing shall be provided |  |  |
| (d) Where audio information is important for the use of a product, at least one mode of operation and information retrieval shall be provided in an enhanced auditory fashion, or support for assistive hearing devices shall be provided. |  |  |
| (e) At least one mode of operation and information retrieval that does not require user speech shall be provided, or support for Assistive Technology used by people with disabilities shall be provided. |  |  |
| (f) At least one mode of operation and information retrieval that does not require fine motor control or simultaneous actions and that is operable with limited reach and strength shall be provided. |  |  |

|  |  |  |
| --- | --- | --- |
| **Section 1194.41 Information, documentation, and support** | | |
| **Criteria** | **Supporting Features** | **Remarks and Explanations** |
| (a) Product support documentation provided to end-users shall be made available in alternate formats upon request, at no additional charge. |  |  |
| (b) End-users shall have access to a description of the accessibility and compatibility features of products in alternate formats or alternate methods upon request, at no additional charge. |  |  |
| (c) Support services for products shall accommodate the communication needs of end-users with disabilities. |  |  |