Sol. W9124D-23-R-0007

Information Technology Support Services (ITSS),   
U.S. Army Recruiting Command, Fort Knox, KY (USAREC)

Due: ~~October 27, 2022 09:00 a.m. ET~~

Submitted by:

HunaTek

**Contents**

Understanding of the Government’s Needs 1

Evaluation Criteria 1

Corporate Information 1

Corporate Experience (1.3) 3

Technical Approach 8

Requirements Specifications (5.2.1) 8

5.2. Requirements Engineering 9

Project Controls (5.9.1) 10

Data Analysis of Business Information (5.16.1) 10

Help Desk/Ticket Resolution/Incident Response (5.20.1) 13

Problem and Event Management (5.20.6) 17

Configuration and Administration of Army and Commercial Platforms (5.22.6.4) 19

5.22. Support the Administration of the IT Workforce Readiness 20

Monitoring (5.24.1) 22

5.24 Network Operations 23

Other Task Areas 25

5.1. Functional Support 25

5.3. Business Process Modeling 28

5.4. Software Engineering 28

5.5. Applications and Web Integration 32

5.6. Data Engineering 34

5.7. Database Management and Administration 35

5.8. Project Management 35

5.10. Software Integration Engineering 37

5.11. Training Support Services for Recruiting and Retention College 39

5.12. Process Improvement 40

5.13. Information Technology Asset Coordinator 40

5.14. Telecommunications Control Officer 41

5.15. Test and Evaluation 41

5.17 General System Support 44

5.18. Computer Graphics 45

5.19. Technical Writers 45

5.21. Information Management Services 45

5.23. Administrative Support 46

5.25. Cyber Security 47

5.26. Monthly Report 48

Quality Control / Quality Assurance 48

Management Approach 53

Approach to Managing Personnel and Deliverables 56

Subcontractor Management 56

Recruiting and Retaining Cleared, Qualified Personnel 57

Staffing Plan (1.2) 58

Security 59

GFI/GFP 63

OCI 64

Transition 65

Submission: 1” margins, 11 pt Calibri font/9pt for tables. Technical capability (Page limit 20 pages)

# Understanding of the Government’s Needs

Objectives: To provide USAREC with ongoing ITSS for the USAREC for joint recruiting services through innovation, responsiveness, flexibility, and reliability while delivering a fully integrated environment supporting anytime, anywhere IT services.

## Evaluation Criteria

|  |  |
| --- | --- |
| Technical Capability - Responses shall be evaluated to assess feasibility of the proposed approach, plans, methods, and managerial ability to perform/manage the work, based on the Government’s assessment of the work. |  |
| Resource Information - Responses shall be evaluated to assess the feasibility of meeting the mission requirements with the proposed staffing plan based on the Government’s assessment of the work. |  |
| Experience - Responses will be evaluated to assess corporate experience with respect to projects similar in scope (tasks similar in complexity to those outlined in the PWS, Part 5) and size (annual value of $3.5 million or greater) to the work described herein. |  |

# Corporate Information

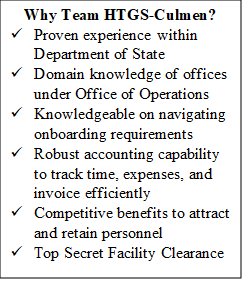
Separate from the non-price factor and price factor, Contractors must provide a cover letter addressing the following:

|  |  |
| --- | --- |
| Company Name | HTGS-CULMEN JV LLC |
| Company Address | 13900 Lincoln Park DR  STE 350  Herndon, Virginia  20171-3264  United States |
| Point of Contract | Michael Torres |
| Phone Number | 202-921-2314 |
| E-mail Address | Mike.Torres@hunatek.com |
| Unique Entity Identifier | SHBNL96ZTBJ7 |
| CAGE Code | 8NZ23 |
| Tax Identification Number |  |
| Supplier Self-Service Pilot (252.232-7998): Y/N | No |

Company Name  
Company Address  
Point of Contact – authorized to obligate the contractor  
Phone Number  
E-Mail Address  
Unique Entity Identifier  
CAGE Code  
Tax Identification Number  
Confirm Yes or No, regarding participating under Supplier Self-Service Pilot (252.232-7998)

Any assumptions, exceptions, or deviations shall be addressed citing specific solicitation paragraph. Acknowledge of all amendments (if applicable) .

Proposal Acceptance Period shall be identified. Proposal acceptance period shall remain valid for a period of 90 calendar days after the closing date and time identified in the solicitation. Proposals offering less than 90 calendar days may be rejected as non-responsive.



HTGS-Culmen JV, LLC, (HTGS-Culmen) is a joint venture (JV) between Culmen International, LLC (Culmen) and Distributed Computing System Solutions Provider, Inc., d/b/a HunaTek Government Solutions (HunaTek), a Small Business Administration (SBA) Certified 8(a) Alaska Native Corporation (ANC)-owned company. Members have an SBA approved Mentor Protégé Agreement (MPA) allowing HTGS-Culmen to qualify as an 8(a) ANC-owned company under NAICS 541512.

This partnership was forged to combine the unique experience and capabilities of both firms to create a robust solution offering to its customers. Sharing a common set of values in how we view management and quality across the full delivery cycle, we maintain a firm commitment to working closely with the US Army Recruiting Command and its stakeholders in aligning contract delivery to Information Technology Support Services (ITSS) requirements.

A brief description of each company (HunaTek, Culmen and The Building People) making up the HTGS-Culmen team is provided below:

**Table 1 - Team Experience & Benefits to State**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Team Member | Experience | Benefits to DoS |  | |
| Picture 2 | **HunaTek**, the Managing Member of HTGS-Culmen, is an ISO 9001:2015 certified company with a TS FCL. It currently holds two staffing IDIQs with combined ceilings of nearly $50M. Its management has supported DoS since 2015 and has supported other staffing IDIQs with ceiling values up to $200M. | * Service-driven business model focused on delivering solutions while utilizing established business processes, project management, and controls that provide measurable metrics. * Direct experience with DoS as a prime contractor supporting similar staff support contracts. | |  |
| Picture 3 | **Culmen** is an ISO 9001:2015 certified company with a TS FCL, a Member of HTGS-Culmen, and HunaTek’s mentor under an approved SBA MPA. Its experience within DoS includes staffing of senior personnel support nonproliferation and disarmament, facilities management, and logistics & procurement worldwide. | * Well versed in deploying personnel worldwide with over 40+ currently deployed and direct experience in 24 countries. * A large company with significant recruiting capabilities and proven success in capturing hard to find candidates. * Proven DoS contractor satisfying large scale requirements. | |  |

## Corporate Experience (1.3)

(2 page limit)

|  |  |
| --- | --- |
| **Organization Name:** | ***U.S. Army Office of the Judge Advocate General*** |
| **Name and Address of Awarding**  **Organization or Agency:** | Ms. Jennifer Rustwick  Contracting Officer  US Army Contracting Command  973-724-6812  jennifer.m.rustwick.civ@mail.mil |
| **Activity Title:** | Office of the Judge Advocate General (OTJAG) Main Information Technology (IT) Support Services (ITSS) |
| **Contract No.:** | W15QKN20C0061 |
| **Programmatic Support:**  Under this contract HunaTek is responsible for maintenance and development of 80+ custom applications and 6000+ databases that make up JAGCNet, the Army JAG Corps internet-based enterprise knowledge management portal. Collectively JAGCNet applications and databases serve over 10,000 end users consisting of Department of Defense (DoD) attorneys, paralegals and support personnel around the globe.  As part of the scope of this contract HunaTek provided a full range of IT support services to include Security/Information Assurance (IA) Assistance, Application Maintenance Services, Strategic Program Management Support, Website Content Maintenance, Network Operations Management, and Help Desk Support Services. | |

**Culmen Past Performance Contracts for USARC ITSS**

|  |  |
| --- | --- |
| **Customer Name:** | **Department of Homeland Security, Network Security Division (NSD)**  ***Program Management Office Support*** |
| **Name and Address of Awarding**  **Organization or Agency:** | OSA CYBER  245 Murray Lane,  Washington D.C. 20528 |
| **Activity Title:** | Programmatic Support/Administrative |
| **Contract No.:** | GS00Q14OADS104 |
| **Order No. (if any):** | HSSA01-17-F1405 |
| **Period of performance:** | 08/30/2017 – 08/29/2023 |
| **Dollar value:** | $79,632,035.93 (Award Value) |
| **Explanation of relevance to the proposed acquisition:** | |
| Culmen International, LLC provides programmatic, communications, and outreach and administrative support to the Department of Homeland Security’s Cybersecurity Infrastructure Security Agency (CISA) that is directly related to the requirements stated in the USARC ITSS PWS. This staffing support contract requires Culmen to recruit, hire, retain staff in non-direct hire positions in support of NSD. Culmen leverages its mature recruitment, hiring and onboarding, and training process in order to maintain provide qualified programmatic and administrative staff to meet all Program Objectives. | |
| **Contact information (names, job titles, mailing addresses, phone numbers, e-mail addresses of the procuring Contracting Officer and/or the Contracting Officer ‘s Representative):** | Emilie Maloof (COR)  Program Analyst, Capability Delivery  Cybersecurity Division  Cybersecurity and Infrastructure Security Agency  Office: 703-235-3059 | Cell: 202-875-1162 | E-mail: emilie.maloof@cisa.dhs.gov |
| **Description of the performance** | |
| **Scope of work or complexity/diversity of tasks:** | |
| **Programmatic Support:** Culmen provides all manner of program office support, including preparing status reports, documentation of office operations using SharePoint, providing strategy and policy guidance to Cybersecurity and Infrastructure Security Agency (CISA) leadership, and all aspects of contract support. Culmen takes government and industry monthly inputs and provides schedule, funding, and milestone analysis to the CORs and government program and portfolio managers. Culmen supports all Program Management Reviews (PMRs), including coordinating logistical support in the scheduling of conference rooms and video teleconferencing (VTCs), documenting action items and providing meeting minutes. Culmen directly supports the Investment and Contacts’ Management Branch in developing a MS Access database to automate and house all financial/budget, cost estimating and contract administration data. CISA leadership is now exporting this database to other divisions to enhance and provide efficiencies of these critical functions throughout CISA. Culmen also provides SharePoint product development and administration services by developing forms to automate procurement processes and develop branch intranet sites to facilitate the storage of documents, enhance collaboration and provide workflow processes. Culmen provides SharePoint services that provide CISA divisions and branches to store and track document-based deliverables and provide a mechanism for government and industry partners to have standardized workflow processes. Culmen also utilizes the CISA Executive Secretary Tasking Tracker (ESTT) system to track documents and taskings to ensure correct promulgation of taskers and to track to completion. Culmen supported all Cybersecurity Division (CSD) and National Cybersecurity and Communications Integration Center (NCCIC) Operations Division planning activities towards the CSD 5-year Strategic Implementation Plan, and Annual Operating Plan.  **Communications and Outreach:** Culmen directly supports CISA through internal and external communications support and outreach to include developing Communication Management Plans and Human Resource (HR) outreach to federal employees. Culmen reviews organization newsletters to ensure pertinent information such as pay, leave accruals and benefits are accurate and up to date. Culmen also researched and provided additional strategic-level electrical grid cybersecurity information to assist the NCCIC Communications Branch in revising talking points for the NCCIC Deputy Director of Operations’ keynote speech. Participated in an Office of Legislative Affairs prep session for a briefing by the Cybersecurity Threat Detection and Analysis (CTDA) Division Chief of Communications Branch to Senate staffers. Culmen provided research support and wrote talking points on NCCIC’s role in relation to the PPD-41, NCIRP, and UCG national policies in support of the briefing. Culmen directly supports the strategic communications mission of the National Security (NSD) and participates in the CISA Employee Engagement Ambassador program.  **Administrative Support:** Culmen provides administrative and technical writing support, including the preparation of publications and presentations of a strategic nature and related to watch-team training. Culmen develops briefings for the purpose of indoctrination of new federal employees, as well as developing Standard Operating Procedures for CISA division operations as well as liaison management. Culmen provides a variety of administrative support to CISA, including acting as Executive Assistants to various CISA leadership, coordinating CISA leadership travel plans and expense reports and manages senior leadership calendars and schedules. Culmen provided support to the CTDA Division Director and Deputy Director. Support provided included scheduling requests, calendar clean up, room changes, logistics, and general coordination for the CTDA division. Culmen updated and maintained unclassified daily binders to include daily calendar and weekly activity reports for DHS NCCIC CTDA Division Chief and Deputy Chief. | |
| ~~The below statements demonstrate Culmen’s ability to provide quality staff programmatic and outreach staff that far exceed the NSD’s requirements and mission objectives.~~  *~~“Mr. Christian Cosans is supporting the Business Operations Branch within the Network Security Deployment (NSD) under the Cybersecurity Division (CSD) of the newly created Cybersecurity and Infrastructure Security Agency (CISA). Mr. Cosans is directly supporting the~~* ***~~strategic communications mission~~*** *~~of NSD and our participation in the CISA Employee Engagement Ambassador program. The Ambassador Program was formed in response to the preliminary 2018 Federal Employee Viewpoint Survey results and seeks to improve work culture within the agency.~~*  *~~I want to highlight a few comments from my staff about Mr. Cosans. “Christian continues to exceed expectations every single day. I can send him a few emails with little direction and he hits the bullseye 90% of the time by completing a task for me and getting it back to me before my assigned deadline. He is intelligent, proactive, and a great communicator. I have been bringing him to leadership meetings with me (the Monthly Supervisor Meetings) and he has been helping me with developing the first draft of policies, the newsletters, agendas, meeting minutes, and he even developed a shared folder for the two of us to keep track of our projects. He's absolutely an asset to NSD.” Ashley Pearce, Official Ambassador for NSD at CISA program.~~*  *~~Personally, I have observed that Mr. Cosans supports our mission requirements in a consistent and professional manner. His courteous and jovial attitude makes our workplace better and we are very pleased with the quality of service Christian provides to the Business Operations branch and NSD in general.”~~*  ~~Alex Morales, GS15~~  ~~Chief, Business Operations~~  *~~“Ms. Karla Dishun is supporting the National Communications Coordination Branch (NCC) within the CISA Integrated Operations Coordination Center (CIOCC). Ms. Dishun's primary task has been updating the work instructions for the COMM-ISAC Watch and then providing/coordinating training on those work instructions for the surge personnel who augment the Watch during major disasters.~~*  *~~On short notice during the Hurricane Dorian crisis, I informed my team we needed the surge role of historian filled as soon as possible. Without hesitation, due to her exceptional quality of work with COMM-ISAC Watch, the team contacted Ms. Dishun to fill this role and worked all the necessary coordination details since weekend and holiday hours were required. Serving as historian, Ms. Dishun participated in four conference calls each day, providing a summary transcript for two of them; the other conference calls were for situational awareness if NCC taskers were issued, she was asked to capture them. The NCC requirement was transcript completion within two hours of the end of the conference calls. Ms. Dishun quickly grasped the task and routinely had summaries ready within 30 minutes of the conference calls. These efforts were extremely noteworthy and "make Ms. Dish..un a valued asset to the NCC team."~~*  ~~John O’Connor Jr.~~  ~~National Communications Coordination Branch~~ | |

# Technical Approach

(a) Describe the technical approach, plans, and methods for completion of the following tasks identified in PWS Part 5. The tasks are representative of some of the more complex tasks performed as part of overall mission requirements. Information provided should be in sufficient detail that it demonstrates Contractor’s technical understanding of the requirements:

(i) 5.2.1 Determine, analyze, and validate detailed requirements specifications.

(ii) 5.9.1 The contractor shall provide support to establish and maintain standardized project controls for Government assigned projects and ensure that project schedules are maintained and integrated into one master schedule.

(iii) 5.16.1 Applies industry-standard strategies and technologies used for the data analysis of business information.

(iv) 5.20.1 Contractor shall provide technical resolution for an average of 4,000-6,000 incident tickets per month (incident volume increases during periods such as system upgrades, network disruptions, and asset lifecycle replacement). Incidents are submitted by approximately 13,000 users located within the USAREC Headquarters building (Fort Knox), Army Marksmanship Unit (AMU) (Fort Benning), Special Operations Recruiting Battalion (SORB) (Fort Bragg), Recruiting and Retention Collage (RRC) (Fort Knox), and across USARECs 1800+ Brigades, Battalions, Companies and Stations worldwide. 80% of incidents should be resolved during the first contact and 100% within 72 hours. Contractor must be capable of serving as subject matter experts (SME) on common and advanced incident topics as described below and liaison with external agencies, vendors and key stakeholders to resolve incidents, problems, and events.

(v) 5.20.6 Problem and Event Management. Contractor shall identify risks, secondary impacts, and systemic problems that are reported from end users, service providers, other agencies, and commercial vendors. Problems should be promptly reported, assigned/escalated to the appropriate resource for resolution, and tracked through resolution.

(vi) 5.22.6.4 Provide configuration, customization, and administration of Army and commercial standard platforms. This may include customizing screens, editing fields, creating workflows, configuring reports, user account management, permissions, and roles, configuring security and privacy settings, and any other functions that would be required to ensure the platforms meet the government’s needs.

(vii) 5.24.1 Monitor network, system and application performance and work with government identified service providers to resolve issues such as outages, service degradation, upgrades, and maintenance. Networks include but are not limited to commercial and government hardwired and mobile networks providing internet, data, voice, fax, and other telecommunications services. Systems and applications include both GOTS and COTS products.

(b) Provide clearly defined management and organization structure and procedures that demonstrate Contractor's ability to manage a requirement of this size (annual value of $3.5 million or greater) and scope (tasks similar in complexity to those outlined in the PWS) as well as quality control matrix that demonstrate Contractor's ability to meet or exceed performance standards.

## Requirements Specifications (5.2.1)

Determine, analyze, and validate detailed requirements specifications

Hunatek will support the requirements management process by involving QA team to identify any ambiguous, not clear, not testable requirements early in the process. We will participate on the Configuration Control Board. We understand this may include, but not limited to, analytical capabilities, infrastructure innovation, data innovation, determining and communicating which requirements are testable, ensuring the quality of the Requirements Traceability Matrix for complete test coverage, and other support as required by the government. Hunatek will engage in practices to enable rapid fielding of capabilities developed externally including the establishment of a Continuous Integration Practice built on the Continuous Integration/Continuous Delivery methodology providing the systematic, repeatable, secure, and streamlined delivery of capabilities to production environments.

### 5.2. Requirements Engineering

The Government will provide needed modification requirements via government-issued actions such as scope documents, requirement documents, change requests, problem reports, and troubleshooting and/or other maintenance tasks related to the sustainment of production systems.

5.2.1. Determine, analyze, and validate detailed requirements specifications.

5.2.2. Perform requirements change management.

5.2.3. Document detailed requirements and design specifications by Government policies, processes, and procedures:

5.2.3.1. Maintain version control of architecture products using approved version control processes.

5.2.3.2. Maintain compliance with Business Enterprise Architecture (BEA) 5.0, and future versions.

5.2.3.3. MaintainarchitectureaccuracycompliantwiththeDepartmentofDefenseArchitectureFramework(DODAF)2.0 and future versions.

5.2.3.4. Maintain the All Viewpoint that describes the overarching aspects of architecture context that relate to all viewpoints.

5.2.3.5. Maintain the Capability Viewpoint that articulates the capability requirements, the delivery timing, and the deployed capability.

5.2.3.6. Maintain the Data and Information Viewpoint that articulates the data relationships and alignment structures in the architecture content for the capability and operational requirements, system engineering processes, and systems and services.

5.2.3.7. Maintain the Operational Viewpoint that includes the operational scenarios, activities, and requirements that support capabilities.

5.2.3.8. Maintain the Services Viewpoint that includes the design for solutions articulating the Performers, Activities, Services, and their Exchanges, providing for or supporting operational and capability functions.

5.2.3.9. Maintain the Standards Viewpoint that articulates the applicable operational, business, technical, and industry policies, standards, guidance, constraints, and forecasts that apply to capability and operational requirements, system engineering processes, and systems.

5.2.3.10. Maintain the Systems Viewpoint that describes the design for solutions articulating the systems, their composition, interconnectivity, and context providing for or supporting operational and capability functions. Must provide updates within 24 hours to Government as changes occur.

Hunatek’s QA and cybersecurity SMEs will assist in reviewing software design documentation provided in application design review periods such as software design descriptions and software requirements specifications. We will examine network diagrams and mock framework designs. For example, Hunatek has found that the UML (Unified Modeling Language) is also another method that can be leveraged for design and definition for design reviews. There are several diagram types within the UML which can be developed at each stage. Informal Peer Reviews are a minimal type of review required for selected software development work products. These peer reviews are planned as part of the original development of any (all) project work product such as SRS, Storyboard, SDD, source code and Integration Test scenarios and scripts. Metrics are collected from each checklist and logged in the Peer Review metrics spreadsheet maintained by the team lead.

## Project Controls (5.9.1)

(ii) 5.9.1 The contractor shall provide support to establish and maintain standardized project controls for Government assigned projects and ensure that project schedules are maintained and integrated into one master schedule. 5.9.1 The contractor shall provide support to establish and maintain standardized project controls for Government assigned projects and ensure that project schedules are maintained and integrated into one master schedule. The contractor shall conduct Project Control activities including:

5.9.2. Integrate project schedules into an integrated master schedule.

5.9.3. Establish dependencies between related project schedules and report potential impacts to ensure accurate schedules and metrics are provided to Government managers.

5.9.4. Develop and maintain common schedule dictionaries to assist in maintaining integrated schedules. 5.9.5. Build and maintain project Work Breakdown Structures (WBS).

5.9.6. Support scheduling meetings and other meetings as appropriate.

5.9.7. Administer the consolidated time tracking tool, currently MS Project Server.

5.9.8. Provide to the Government earned value, cost and schedule analyses, and ad hoc reports.

5.9.9. Provide training on developing and maintaining project schedules as required and when requested.

For the this program, Hunatek will load all supported organizations and associated CLINs into our project management tool, create the work breakdown structure (WBS), and then develop the Authorized Position List assigning each position to a WBS element resource using the allocation matrix and the resource calendar. We add all project deliverables using the PWS requirements. Our project management tool then creates the schedule baseline by which we monitor performance and associated risks.

By using labor and rate application tables, our project management tool applies costs to create the baseline budget and associated cost and funding schedule to enable cost tracking. Hunatek uses a Project Controller Specialist (indirect) as the primary controller, which ensures consistency and efficiency of application performance to support each task. A Project Controller Specialist assists the PM and task leasds in monitoring cost and schedule throughout contract execution.

## Data Analysis of Business Information (5.16.1)

(iii) 5.16.1 Applies industry-standard strategies and technologies used for the data analysis of business information. The contractor shall:

5.16.1. Applies industry-standard strategies and technologies used for the data analysis of business information.

5.16.2. Plan and execute software installations, upgrades, and configurations for Business Intelligence tools.

5.16.3. Visualize data using a variety of methods such as reports and dashboards to support smart business decisions.

5.16.4. Perform data analysis and data modeling to identify historical, current, and predictive trends and insights of business operations.

5.16.5. Business Intelligence specific proficiency in MS Office applications such as Access and Excel; query languages such as to SQL; commercial BI applications such as Power BI; and cloud environments such as Army 365 and Azure.

5.16.6. Administration and maintenance of Army data analytics system of record.

5.16.7. Inspect & Assess data sources and databases.

5.16.8. Collaborate with the government to address BI Project needs. Translate business requirements into a business dimensional model, key subject areas, dimensions, hierarchies, attributes, and measures.

As digital transformation is changing the way government is responding to disruption, Hunatek's Government Services is focused on short-term and long-term initiatives to help these organizations navigate this transformation. Our short-term focus is on two areas of the digital government experience: the citizen, also considered the consumer of government services and the digital government worker. We are focused on looking across the holistic digital worker-to-digital citizen experience not just the immediate touch points or needs.

The second area we look at is dense or complex data and making it more consumable and actionable. This means digitally transforming any really large amount of data, whether it is health research or fixed survey data like commerce, and putting it into a consumable format across digital distribution channels; thereby, creating real, translatable value for specific audiences.

Finally, the third area involves extending the service paradigm. Historically, we’ve seen the emphasis on infrastructure improvements, such as the cloud. I’d like to see that concept and paradigm extended into service-as-a-service so the pricing of government services are based on results or outcomes as opposed to level of effort. Longer term, we believe that government and public service has to be more proactively personalized. With our experience in the commercial and nonprofit space, we understand how to link and create personalized public service across all layers of that delivery chain.

Data Warehouse and Business Intelligence

The solutions to challenges of federal agencies are hidden within the large stacks of data that governments have gathered throughout the years. Business Intelligence helps them structure the data into meaningful, insightful and valuable information within an automated environment. It provides them easy access to the answers they are looking for by analyzing trends concealed in hundreds of millions of records. Different tools help them to answer ad-hoc questions, create structured reports, provide the numbers for their annual reports and have dashboards to follow up on their goals and actions.

Hunatek's Data Warehousing and Business Intelligence (DW BI) implementations provide a very strong and deep rooted foundation based on substantial experience, enterprise performance management, considerable technological consulting, proven implementation frameworks, readymade solutions and accelerators, and effective knowledge management. Team Brite, in partnership with industries leading Business Intelligence solution vendors including Informatica, Microsoft, and Oracle fully exploits the product features and enables faster implementations thus delivering tangible business benefits to our customers across industry verticals.

We have developed complex operational reports, management dashboards, and data visualization solutions for agencies in support of simple and complex analytics requirements. Optimizing the performance of complex reports that sift through millions of records of data utilizing Extract, Transform, and Load (ETL) strategies that compile operational data from numerous systems and data sources using agency standard tools has been an integral part of our implementations. In additional to traditional means of data warehouse analysis the government has also started investing in big data and unstructured forms of data analysis. Team Brite has been in the forefront of the technological advances and has helped multiple agencies with their big data strategy and proof of concepts.

Data Mining

Data mining is an effective set of analysis tools and techniques used in the decision support process. The federal agencies are dealing with the onslaught of vast amounts of valuable data and are planning to use, data-mining programs for scores of activities ranging from improving service, performance, and human resource management to analyzing intelligence and uncovering several new fields of research in bio science and other related areas. At its core, the Data mining process involves analyzing diverse data sources in order to identify relationships, trends, deviations and other relevant information that would be valuable to an organization. Team Brite understands the challenge that the government agencies face while analyzing large amounts of data and being able to derive meaningful insights. Our team has implemented several techniques that enable predictive analytics and advanced modeling on raw data collected from various sources. Team Brite has been involved with the Census Bureau and Department To help mine large amounts of unstructured and raw survey data to gain valuable insights about the population. We have helped established a platform for analytics and mining big data at the Bureau that allows survey statisticians perform concurrent analysis and estimation using a variety of technologies such as SAS, R and Python over a Hadoop based platform for analytics.

Knowledge Management

Knowledge management for federal programs enables a cultural shift — so that agencies capture, retain, share and reuse information to build, maintain and support a collaborative, learning organization. In simplest terms, the KM process can be summarized through three steps: Capturing ► Retaining ► Learning.

Knowledge capture focuses on the cultural emphasis to store information in a centralized repository for the basis of collaboration and process improvement. Knowledge retention does not simply revolve around data capture and centralization; rather, it keys on a commitment within the organization to share meaningful information. The transformation of knowledge capture and retention into business agility, growth, and optimization constitutes learning.

Technology is a key enabler of knowledge management and communities of practice. Team Brite has been successfully implementing knowledge management solutions for agencies and our focus has been around best practices in the following areas of knowledge management -

KM Technology Architecture: Development of a formal plan and design for KM technology implementation and operation within an organization.

KM Net Portals: A Web application that provides an entrance point into KM databases, systems, and tools.

Online Expertise Directories: A web-based application that enables users to access a listing of staff that identifies their knowledge, skills, and abilities.

Facilitated CoPs Online: Web-based portal that provides access to CoP and is monitored by dedicated staff.

Electronic Document Management: Systems that manage the process of document production, revision, and release. Typically, they incorporate a central database and networking software. Usually the document database is accessible over a local area network and is used to store all documents for a specific project, division, or organisationz.

Collaborative Software: These groupware refers to programs that help people work together collectively while located remotely from each other. Groupware services can include the sharing of calendars, collective writing, e-mail handling, shared database access, electronic meetings with each person able to see and display information to others, and other activities.

eLearning: Knowledge management can significantly enhance the organization's learning program and should be integrated together.

## Help Desk/Ticket Resolution/Incident Response (5.20.1)

(iv) 5.20.1 Contractor shall provide technical resolution for an average of 4,000-6,000 incident tickets per month (incident volume increases during periods such as system upgrades, network disruptions, and asset lifecycle replacement). Incidents are submitted by approximately 13,000 users located within the USAREC Headquarters building (Fort Knox), Army Marksmanship Unit (AMU) (Fort Benning), Special Operations Recruiting Battalion (SORB) (Fort Bragg), Recruiting and Retention Collage (RRC) (Fort Knox), and across USARECs 1800+ Brigades, Battalions, Companies and Stations worldwide. 80% of incidents should be resolved during the first contact and 100% within 72 hours. Contractor must be capable of serving as subject matter experts (SME) on common and advanced incident topics as described below and liaison with external agencies, vendors and key stakeholders to resolve incidents, problems, and events. 5.20.1 Contractor shall provide technical resolution for an average of 4,000-6,000 incident tickets per month Incidents are submitted by approximately 13,000 users located within the USAREC Headquarters building (Fort Knox), Army Marksmanship Unit (AMU) (Fort Benning), Special Operations Recruiting Battalion (SORB) (Fort Bragg), Recruiting and Retention Collage (RRC) (Fort Knox), and across USARECs 1800+ Brigades, Battalions, Companies and Stations worldwide. 80% of incidents should be resolved during the first contact and 100% within 72 hours. Contractor must be capable of serving as subject matter experts (SME) on common and advanced incident topics as described below and liaison with external agencies, vendors, and key stakeholders to resolve incidents, problems, and events.

5.20.1.1. Common USAREC desktop support incident tickets may include: IN/OUT Processing, Asset Management, Provisioning User IT Equipment, Networking and Connectivity, Software Licenses Management, Entitlement Management, Account Management, Printer Configuration and Networking, Hardware/Software Troubleshooting, Email/Mailbox/Distribution List Requests, Secure Host Baseline (SHB)/ Operating System Issues, A365 and other Cloud Platform Issues, Government/Commercial Systems and Applications, IT Hardware Repair, and Providing Basic IT Support and User Training.

5.20.1.2. Common USAREC biometric (fingerprinting) support incident tickets may include Hardware/Software troubleshooting, Account/License/Entitlement Management, Hardware Provisioning, Asset Management, Assisting the Field in Obtaining Missing Reports, Facilitating Approval for Waiver/Exception Requests, Individual and Group Training on the Use of Biometric Technology.

5.20.1.3. Common USAREC mobility support incident tickets may include Mobile Device Provisioning/Configuration, Mobile Device Management (MDM), Security Compliance, Account Management, Number Porting, Asset Management, Coverage Issues, New Technology Implementations, Mobile Security, Mobile Applications.

5.20.1.4. Common USAREC cyber support incident tickets may include New User Accounts in various GOTS and COTS applications/systems, ATCTS, ACAS, Social Media Threats, VIP reports, CAC Registration, General Cyber Inquiries, User Violation Notices, Investigations, Requests for Information, Certifications, and training.

5.20.1.5. Common USAREC information management incident tickets may include Requests for Business Cards, Freedom of Information Act (FOIA) and Privacy Act inquiries, and Army Records Management requests.

5.20.2. Contractor shall provide troubleshooting, account management, software updating, and imaging for over 140 computer systems for Army Marksmanship Unit (AMU) located at Ft Benning, Ga. The technician will be responsible for keeping computer systems performing in a global environment. The technician will also be responsible for troubleshooting complex target systems to ensure the team can practice before all competitive shooting matches.

5.20.3. Contractor shall provide troubleshooting, account management, software updating, and imaging for over 45 computer systems for Special Operations Recruiting Battalion located at Fort Bragg NC. 20 computers are globally dispersed throughout CONUS AND OCONUS locations. Travel may be required for emergencies. Computing systems are vital to the SORB mission of providing Soldiers with the essential missions as determined by Congress, the Department of Defense, and the Army leadership.

5.20.4. Contractor shall provide help desk technicians for troubleshooting biometrics systems (physical and digital identification) within the command. The Department of the Army mandates the physical and digital identification of all potential enlistees. Biometric systems are prone to have technical issues thus a technician is warranted. Physical and digital identity is vital to the Army to eliminate known criminals from entering the Army enlistment process before expending millions of dollars on unqualified applicants. The Army is missioned to enlist upwards of 80,000 applicants every year. To get the number of applicants needed, recruiters will process upwards of 200,000. All applicants must have biometrics on file to determine moral qualifications before or after enlistment. This position is vital to ensure software and equipment issues are resolved expeditiously to keep the flow of applicants flowing through the arduous process. Technician receives, on average, 20-30 tickets per day.

5.20.5. Create and maintain knowledge articles related to incidents.

When one of USARC’s 13,000 users contacts the USARC Help Desk, HTGS-Culmen JV Help Desk Experts apply an integrated ITIL based service delivery approach to ensure rapid and thorough resolution of concerns as well as customer satisfaction with USARC service. Our Enterprise Help Desk methodology integrates controls for performance and quality management into a cohesive approach ensuring consistency across the task areas of IT Support Services including continuous customer satisfaction delivery. We bring over XX years help desk experience at the <<XXX insert experience here>>. We use ITILv4 Continual Service Improvement (CSI) processes that are mature and repeatable for the USARC, as proven by our ISO-9001:2015 Quality certification and CMMI L3 accreditation for Service. We have used various service desk tools for ticket tracking and analysis, and our process will adapt to the USARC helpdesk tool and processes. ***Upon contract award, we will tailor our ITIL based continuous service delivery approach to meet the specific USARC Service Level Agreements, improve customer service, and immediately address any risks.***

We currently manage a help desk using an ITIL model that supports military, civilians, and contractor users both CONUS and OCONUS with Tier I – IV support for DTRA.

Our industry leading ITIL and ISO best practices for exceptional help desk service are dynamic and adapt to changing USARC needs. A highlight of our best practices are listed in the table below.

|  |  |
| --- | --- |
| **Best Practice** | **Key Elements of HTGS-Culmen JV Help Desk Best Practices** |
| **Measuring, Reporting, & Trend Analysis of Help Desk Metrics** | * Ticket volume, Call volume after a release, Ticket Completion, Open tickets/backlog * Response Time (between ticket creation & first response), Mean Time to Resolution (MTTR), First contact resolution rate (percent solved within first session), Escalation Report, Re-Opened Service Requests * Priority of concern, Type/Category of concern, Type of Contact (email, phone), User group * Customer satisfaction per call for resolution, for help desk staff (segregated by user group), periodic surveys * Identification of trends and impacts across systems, customers, end-users, vendors. * Dashboard and Analytics of SLAs and Metrics, Root Cause Summary Help Desk Report |
| **Integrated Team** | * Capture Help Desk user feedback, analyze ticket contents, and integrate the feedback into the operations and development life-cycle to deliver feedback to PM, Training Team, Change Advisory Board. |
| **Customer Focused** | * Customers know status at all times. Follow-up with customers. * Self-service options where possible * Represent customer feedback to improve system to PM, Application Owners, Change Advisory Board, IT Staff, Trainers * Prevention focused |
| **Knowing Our Customer** | * Deliver tailored service. (Our team brings over XX years of dedicated support to the Army and your mission areas.) * Analyze previous ticket history, user background information, and CRM data to look for trends and patterns so we can adapt our Help Desk experience to each unique USARC user need. |
| **Knowledge Management (KM) Practices** | * Encourage our help desk experts to contribute to KM resources through good ITSM-based KM practices to help capture institutional knowledge and deliver quick and consistent service. * Train our experts to ask the right questions and turn to knowledge resources including previous tickets as a first step toward resolutions. * Check user histories for previous guidance and observations and archive historic knowledge base articles for new rollouts and existing applications. * Incentivize innovation and resolution at first contact. |
| **Maximizing Use of Software** | * Maximize use of USARC ticket management tool and adapt our processes to client tool while leveraging proven methodology to have clear ownership of tickets and tasks, metrics, and reporting. * Recommend alternative approaches to existing process and tools, if cost-effective or desired by USARC. |
| **Configuration & Change Management Practices** | * Good Change Control and identification of Configuration Items (CI) across all phases of SDLC starting from requirements tracking to deployment and operations. * Apply a structured change management process. * Communicate frequently and openly about changes. |
| **Incident & Problem Management**  **Practices** | * Proactive Problem Management to identify & resolve issues before end users report incidents. * Identify patterns * Implementing continuous improvement through reporting of KPIs |

**Systematic Root Cause Troubleshooting**. As a first step in troubleshooting, our Help Desk Technician will consult our comprehensive Help Desk Knowledge Guide for cause and solution steps if a solution is not immediately obvious. The guide provides lines of questions for uncovering common issues and provides steps for resolution. The majority of the time, solution for the incident is identified at this point using our comprehensive Knowledge Guide, resulting in first touch resolution for USARC end users to continue performing duties. In cases where further investigation is necessary to discover the root cause as part of problem management, our Help Desk Technician will lead appropriate Tier II/Tier III team members (system administrators, quality assurance testers, database administrators, developers, information assurance specialist, Subject Matter Experts (SMEs)) to systematically analyze and isolate root causes for the problem.

**Ensuring the isolated issue is resolved.** After isolating the issue, a solution is tested and then provided to the user. If the solution involves a USARC system change, a change is initiated per change management and configuration management protocols, tested, and released. We create testcases to ensure we replicate the user’s issues. We ensure our testcase passes before releasing the fix. We will follow-up with the user to ensure the issue we isolated is resolved and that they are able to perform their work duties using USARC systems. If unresolved, we modify the test and run through the process again. SUpon resolution, we update documentation for each ticket, close the ticket, collect customer feedback, and add to Help Desk Knowledge Guide when relevant.

**Hours.** Help desk will be available <<insert days, hours here if know, otherwise remove>>>. HTGS-Culmen JV ITIL Service Methodology ensures smooth hand-off, real-time status of all issues, and consistent processes for seamless shifts among help desk personnel. For instance, procedures will require date and time stamp to accompany all actions on a ticket, action documentation will have particular minimum requirements for the type of issue, each ticket will be assigned a category type, status and priority.

**Help Desk Guide**. We will create a Knowledge base repository and Help Desk Guide with answers to commonly asked questions, instructions to resolve common users issues, “how-to” instructions to use new features, Operations Procedures including guidance for questions to best define the problem and solutions to common technical issues. Typically, we create this as an internal Wiki to continual update and improve. The USARC Help Desk Guide will be updated for major releases and upon trend analysis of common issues.

**ITIL Continuous Service Improvement (CSI) based Methodology**. HTGS-Culmen JV process provides consistent service based on industry best practices for service focused on continual improvement. Proof of continual improvement is measured through metrics**.** Our personnel will demonstrate the upmost in professionalism in their interactions with USARC customers, and will pay attention to quality details, such as mandatory Auto Spell Check of responses to tickets.

**Metrics**, **Analysis, and Reporting.** The metrics below are common metrics we track to analyze trends and modify processes to continuously improve service. Based on our initial analysis of USARC helpdesk data and the Help Desk, or after trend analysis during the contract, we may add additional metrics to incentivize service level improvements.

* Ticket volume, Call volume after a release, Ticket Completion, Open tickets/backlog
* Response Time (between ticket creation and first response), Mean Time to Resolution (MTTR), First contact resolution rate (percent solved within first session), Escalation Report, Re-Opened Service Requests
* Priority of concern, Type/Category of concern, Type of Contact (email, phone, walk-in), User group
* Customer satisfaction per call for resolution, for help desk staff (segregated by user group)
* Customer satisfaction periodic surveys that capture satisfaction with performance and Help Desk

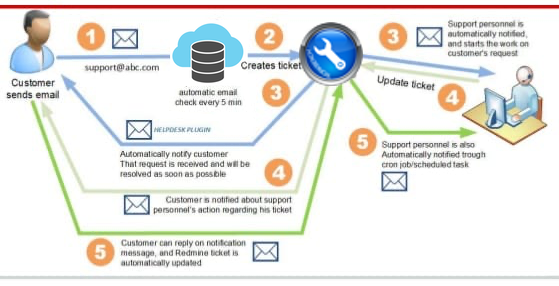
It is our assumption the USARC helpdesk tool has the built-in capability to report on many of the metrics (customer satisfaction with the support, customer satisfaction will Help Desk Technician (by name), type of contact (i.e., e-mail, phone, walk-in), number of contacts, area of concern, and unit of customer making the contact. Those Metrics will be delivered consistently to the COR as required (report formats we have used include dashboards, graphs, and charts. HTGS-Culmen JV will report SLAs and resolve 80% of incidents upon first contact and 100% within 3 business days of initial contact. Wewill identify and recommend any additional metrics or processes. If the COR desires to see those with the bi-weekly report, that can be arranged, or we can establish a monthly or quarterly review of some of the more in-depth metrics, providing more detailed insights to improve performance without providing additional burden on the COR.

***Upon contract award, we will tailor our industry leading ITIL based continuous***

***delivery approach to meet the specific USARC SLAs, improve customer service, and immediately address any risks***.

## Problem and Event Management (5.20.6)

(v) 5.20.6 Problem and Event Management. Contractor shall identify risks, secondary impacts, and systemic problems that are reported from end users, service providers, other agencies, and commercial vendors. Problems should be promptly reported, assigned/escalated to the appropriate resource for resolution, and tracked through resolution.

Hunatek’s Support Services clearly defines how we will meet the requirements of the PWS, more specifically: provisioning users, configuring the software solution, deploying into the AWS FedRAMP-compliant environment, and continual end-user Tier 1/2 support. As part of our comprehensive support, Hunatek will troubleshoot and report on any system failures and performance or security issues. As part of our COOP, we will provide data backup and recovery. Covered under information assurance (IA) and cyber security, we will monitor network communication, patch systems with latest security updates, and monitor logs for performance and security issues. As part of systems support and administration, Hunatek will update systems with new versions of application software, provide documentation of system changes and updates. We will implement federal, DOE policies as directed. Our management approach explains how we will provide monthly status report on work accomplished with hours performed per task, as well as Weekly Activity Reports.

Operations Center Support — Hunatek will provide 24/7 (365 days a year) watch for the SAAS offering’s Operations Center (OC) dashboard at Amazon’s FedRAMP-certified deployments. This support requires routine shift work during non-standard duty hours (1700 hrs to 0800 hrs) and regularly scheduled weekend shifts. Hunatek will assist in the coordination of outages and maintenance, as well as for contingencies and crisis situations. Hunatek will review and analyze all cyber situation reports and other issues that could impact up-times. We will make a concise substantive reporting recommendation to the government when required. Hunatek (watch) personnel will use our knowledge management and service support tools, such as our Automated Message Handling tool.

Service Desk Support — Hunatek will provide tier 1 and 2 end user support. Further, we will provide systems engineering support to enable updates to the onboarding and recruiting system. Using our ITIL-based Service Desk approach, we will support our SAAS onboarding and recruiting system, for end user support, systems maintenance, and cyber security. We will provide a Contractor’s Progress, Status and Management Report to keep the COR apprised of significant events and issues, monthly. We will attend any meetings (virtually) as required. We will provide training support for end users and administrators of the SAAS application. Hunatek utilizes a centralized ticketing, hardware tracking and issue management system that supports user and hardware problem resolution and distributes general information concerning security updates and group policies.

Hunatek will support and assist with systemically tracking engagements with end users and government stakeholders, capturing the results of those engagements and measuring effectiveness. Hunatek will develop and utilize the ATS tool to capture the relevant data necessary to reach prospective employees through multiple communication platforms. We will provide over-the-phone support.

| **Exhibit: Ticket SLA Matrix** | | | |
| --- | --- | --- | --- |
| Severity Level | Response Time | Description | Resolution Time |
| Critical | Within 30 minutes | Complete outage, multiple users impacted, no immediate workaround | Within 8 hours |
| High | Within 2 hours | Degraded service, multiple users affected, latency issues, unable to log into systems | Within 12 hours |
| Medium | Within 24 hours | Does not immediately impede mission performance, only one user affected, work arounds exist, break/fix request | Within 3 business days |
| Low | Within 1 business day | Equipment upgrade, move, new component or enhancement. Impact is low and work can be scheduled based on business case | Within 7 business days |

Hunatek has provided over-the-phone technical support on systems similar to those installed at the government to other customers including multiple Federal Agencies on dispirit projects within the past 5 years. With the collection of data from the help desk tool, and subject to Government review and approval, Hunatek will:

* + Measure the effectiveness of engagements using the data collected;
  + Recommend appropriate techniques and methods within the general scope of statistical analysis to support quantitative studies, recommendations and management decisions;
  + Assist in providing statistical analysis and other support on the overall program and engagement mission. This will include trend analysis, quantitative/qualitative studies, risk analysis, model building and recommendations to assist in management decisions;
  + Execute technical analysis, reports documentation, graphics and publication services in support of program and engagement activities.

## Configuration and Administration of Army and Commercial Platforms (5.22.6.4)

(vi) 5.22.6.4 Provide configuration, customization, and administration of Army and commercial standard platforms. This may include customizing screens, editing fields, creating workflows, configuring reports, user account management, permissions, and roles, configuring security and privacy settings, and any other functions that would be required to ensure the platforms meet the government’s needs.

As to how Hunatek will maintain and update government developed software, COTS software configurations, and software systems (which are geographically separated), we propose undertaking the phases described in the following process enumeration.

Identification & Tracing - This involves activities pertaining to the identification of modifications or maintenance requirements. This can be generated by the user or system and be reported via logs or error messages. This is where we can classify the maintenance type.

Analysis – Any proposed modifications are analyzed for its impact on the system including safety and security implications. If probable impact is severe, alternative solutions are considered. A set of required modifications are then materialized into requirement specifications. The cost of modification/maintenance is analyzed and estimation is concluded.

Design - New modules, which need to be replaced or modified, are designed against requirement specifications set in the previous stage. Test cases are created for validation and verification.

Implementation - The new modules are coded with the help of structured design created in the design step. Every programmer is expected to do unit testing in parallel.

System Testing - Integration testing is done among newly created modules. Integration testing is also carried out between new modules and the system. Finally the system is tested as a whole, following regressive testing procedures.

Acceptance Testing - After testing the system internally, it is tested for acceptance with the help of users. If at this state, user complaints some issues they are addressed or noted to address in next iteration.

Delivery - After acceptance test, the system is deployed either by small update packages or a fresh installation of the system. The final testing takes place on the client end after the software is delivered. Training facility is provided if required, in addition to the hard copy of user manual.

Maintenance management - Configuration management is an essential part of system maintenance. It is aided with version control tools to control versions, semi-version or patch management.

The overall process for software updates includes four main operational phases: synchronization, compliance assessment, deployment, and monitoring. The synchronization phase is the process of synchronizing the software update metadata from the vendors’ update recommendations, and inserting those into the CM process. The compliance assessment phase is the process that where we scan for compliance of software updates and report the compliance state for the software, OS and platform updates. The deployment phase is the process of manually or automatically deploying the software updates to clients. Finally, the monitoring phase is the process of follow-on monitoring for software update deployment compliance.

Finally, the Hunatek approach will facilitate transfer of software products and systems to new users, new machines, or even new support teams. Of course Hunatek’s outputs will serve as a basis for enhancement. Our task outputs are aimed at the product, but not the project that developed it, this serves as a basis for later enhancement. Our work products, not needing to be altered, provide a foundation for continued production evaluation and improvement.

### 5.22. Support the Administration of the IT Workforce Readiness

5.22.1. Maintain up-to-date records, including organizational charts, of IT workforce readiness, including authorizations, filled and vacant positions, in and inbound and outbound personnel.

5.22.2. Maintain up-to-date records of IT certifications across the workforce.

5.22.3. Monitor sources such as the Digital Technology Career Field website and Army Career Program 34 website to identify training opportunities for the IT workforce.

5.22.4. Support maintenance of position and job descriptions.

5.22.5. Serve as SME and supports the management and review of policy and procedural compliance of USAREC IT information systems.

5.22.6. Administrate digital content on Army and commercial standard platforms.

5.22.6.1. Using Army and commercial industry-standard platforms, such as Army 365, to support business processes and create assets, including team sites, pages, lists, libraries, calendars, and workflows. System Support Services

5.22.6.2. Provide account management support.

5.22.6.3. Maintain Command-wide channels to collect, disseminate, and communicate training, policy, procedural, and organizational updates.

5.22.6.4. Provide configuration, customization, and administration of Army and commercial standard platforms. This may include customizing screens, editing fields, creating workflows, configuring reports, user account management, permissions, and roles, configuring security and privacy settings.

5.22.6.5. Provide support services for the test, evaluation, and implementation of new and emerging web-based server services and technologies.

In carrying out this task, we are focused on specific outputs, work products, and other artifacts.Hunatek will maintain and update government developed software, COTS software configurations, and software systems. We will implement software configuration management (CM) procedures to provide a uniform approach to supporting TRIMS, RIMS, IEMS, and other government developed software packages. We will assign a software configuration manager to educate organization stakeholders on CM “best practices,” develop and maintain CM procedures and work instructions for each product assigned. Hunatek will establish release baselines and work with the development teams of GOTS products to administer CM repositories. The Hunatek process for maintaining and updating software includes the development and maintenance of artifacts following proper version control procedures using CMMI-L3 compliant CM processes and work instructions. We will work with the NSWC Corona governing body for reviewing and approving change requests under CM procedures and work instructions.

Maintaining and updating software, whether government-developed or commercial-off-the-shelf applications, requires well-documented configuration management processes, patch management, and version control. Understanding what applications are in the environment is the cornerstone, and Hunatek will update the government’s inventory of applications, ensuring accurate information about licenses, deployment environments, versions, known vulnerabilities, and the user base for each. For example, IEMS uses TRM Rules Manager as a Configuration Control Center for Maximo. In our experience, the Rules Manager Engine provides configuration access to the Maximo Business Object (MB0) and Maximo Integrated Framework (MIF) architectures at run-time. We can implement a collection of services that enables flexibility to configure Maximo, without impacting the out-of-box Maximo code base. Further, Hunatek's expertise with Microsoft Office SharePoint Server will be instrumental in supporting any Web collaboration efforts.

As part of our ISO 9001:2008 approach, the onsite team of engineering technicians and programmers will work with together to ensure they are following proper version control procedures defined in a CM Procedures Handbook we will develop, which maps O&M and CM work instructions — to verify that only CM-approved deliverables are installed into the test environment(s). The main output will be a documented configuration management process, utilized over the lifespan of the effort.

In carrying out System Support Services, our team understands the interrelationship between activities, outputs and the artifacts that are part of this tasking. For example, while our DBA and programmers may have access to the database definition, we may allow some users restricted access so they may execute database queries. These users typically will not have access or the skills necessary to read and understand a database definition. We will provide them with documentation that will help them create their database queries. In collaborating with the client, design reviews are paramount. Not all participants in a design review are going to have the same level of database knowledge and expertise. Subject matter experts may not be technical at all. To facilitate such a design review, we will provide documentation that anybody can read and understand.

We will undertake database design implement our best practices. This mean we will address naming conventions, as the lack of naming conventions can result in very inconsistent and cryptic names for the tables, columns and other database objects, making it difficult to document properly. Applying good naming conventions to the database design will promote better readability of the documentation. We will determine if every table should have a primary key that defines which columns uniquely identify a record; this can improve database performance and data integrity, and is key to understanding the data model. Another important aspect of RDBMS design is understanding the data model by documenting the relationships between tables. The output will be Database Design Documentation.

Hunatek will update and maintain systems, languages, and application software. Typically, Hunatek administrators will not perform the preparation phase on production servers. Rather, administrators or developers create packages or repackage software for Software Installation and Maintenance on test or QA computers. For example, At NSWC, Windows systems would require administrators to use Group Policy to set the scope of management for software installation; this determines which users or systems will get the software patches and upgrades. Using DoD guidelines for SRS developing means we can both define a great specification and help identify deficiencies in past efforts. Hunatek uses the IEEE source for definitions of System and Software Specifications. As designers of high-performance system software, we use IEEE STD 830-1998 as the basis for the SRS unless specifically directed otherwise. We have found that having an excellent SRS is implementing a good SDD, and we use the equivalent IEEE standard STD 1233-1998. The primary deliverable will be the Software Requirements Specification.

The SRS, SDD and other artifacts, in our experience, will address important facets of the solution. They will capture the functionality, hat is the software supposed to do. We will work to document external interfaces, to show how the software interact with people, system hardware, and other software. Because Hunatek solutions architects aim for performance, we want to define what the speed, availability, response time, recovery time of various software functions, are. Naturally, we address other attributes, such as portability, maintainability, and security considerations? The outputs of the Software Design Description documents design constraints imposed on an implementation, and address required standards in effect, implementation language, policies for database integrity, resource limits, operating environment(s), etc.

To build out a complete Software Development Plan, our team strives to achieve a set of characteristics that meet IEEE standards, and result in an approach to the SDLC that is efficient in code development, and effective in project execution. Of course we want the SDP to be correct, but the discipline is keeping the specification up to date when the team find things that are not correct. Our plan, as demonstrated in the attached SDP, results in an unambiguous approach because every requirement stated therein has only one interpretation. This makes our SDP complete and consistent within itself and consistent to its reference documents. Processes we document in the SDP means we can ensure connecting the requirements in the SRS and SDD to higher levels, answering the all-important question, why do we need this requirement?

Hunatek views team collaboration in the software support services as paramount to success; since collaboration is key to NSWC Corona mission success, we will establish a project site with the technical infrastructure needed for collaboration for each task. We can participate in configuration control board meetings with the government to coordinate inter/intra command IT matters and set goals and priorities for projects. The project site (in SharePoint) will enable the shared access to software tools, process maps and SOPs, test suites, and documentation (including user, installation, administration, and design documentation), though the details of how these occur will vary between projects. DoD refers to this technical infrastructure as the set of “data repositories” (see DFARS 227.7108), but the need for collaboration means that these repositories may implement additional requirements not always mandated by contract. Hunatek has learned the lesson that it must be possible for all potential contributors and users to access the tools easily. For example, if security restrictions make it too difficult for people to participate, they will not participate. SharePoint is common at the client facility, and works well with any standards-compliant web browser. Our team also will participate in configuration control board meetings with the government

## Monitoring (5.24.1)

(vii) 5.24.1 Monitor network, system and application performance and work with government identified service providers to resolve issues such as outages, service degradation, upgrades, and maintenance. Networks include but are not limited to commercial and government hardwired and mobile networks providing internet, data, voice, fax, and other telecommunications services. Systems and applications include both GOTS and COTS products. (b) Provide clearly defined management and organization structure and procedures that demonstrate Contractor's ability to manage a requirement of this size (annual value of $3.5 million or greater) and scope (tasks similar in complexity to those outlined in the PWS) as well as quality control matrix that demonstrate Contractor's ability to meet or exceed performance standards.

Our value proposition to the government is Hunatek's ability to be a single point of accountability for service development and delivery across the WAN, LAN, SAN (FC) and Converged network environments (both physical and software defined as depicted in the below diagram) while managing the reference architecture and controlled operation in compliance with federal requirements. This enables the government in return of measurable IT value and our commitment to providing continuous service improvement.

A common way of characterizing network management functions is FCAPS—Fault, Configuration, Accounting, Performance and Security. The Hunatek team will provide network operations, event monitoring and management, performance monitoring, and analysis services. These services provide the capability for centralized operations, monitoring, management and analysis of network systems, core services, as well as network infrastructure assets to include trunks, circuits, routers, switches, cryptologic equipment, etc., 365 days a year, 24 hours per day, 7 days per week.

Hunatek's Network Engineering solution is an innovative combination of sophisticated management tools and services that span the entire network and application lifecycle: planning, design, implementation, and operations (PDIO). Our approach redefines how enterprises can monitor and manage application performance and network services to support business initiatives. This approach addresses many engineering questions to bridge the gap between application and network management, bringing visibility to the interactions between the application and network layers. It extends network management beyond faults and delay metrics to determine whether network resources adequately enable optimal performance of applications and network services. The solution relieves IT staff by automating many necessary, yet tedious tasks. It also shortens planning and deployment times and delivers greater confidence in successful results.

Key benefits to the government include:

* + Helps enable the government to predict the impact of new applications and new network services on existing infrastructures and services prior to deployment
  + Reduces risk prior to application or network service deployment
  + Optimizes network performance by identifying behavioral insights into network and application configuration issues and recommending corrective actions
  + Facilitates faster problem identification and resolution through more granular monitoring and wider visibility
  + Single-vendor advantages: single-vendor integration, single-vendor support

### 5.24 Network Operations

5.24.1 Monitor network, system and application performance and work with government identified service providers to resolve issues such as outages, service degradation, upgrades, and maintenance. Networks include commercial and government hardwired and mobile networks providing internet, data, voice, fax, and other telecommunications services. Systems and applications include both GOTS and COTS products.

5.24.2 Plan system and network maintenance events with service provider and USAREC functional leads to ensure minimal disruptions to Recruiting operations.

5.24.3 Create, manage, ensure compliance and report against Army, TRADOC, and USAREC operations orders, taskings, etc.

5.24.4 Lead, plan, represent USAREC interests in coordination meetings with service providers, industry partners and other stakeholders.

5.24.5 Maintain communications channels with subordinate units and other staff sections.

At Hunatek, the approach we take is based on our history with telecoms and network services. This approach is to capitalize on the efficiency gains of unified communications, cloud computing and convergence/virtualization. Team Hunatek supports network administration for both LAN/WAN; update /change configuration files, hardware and firmware refresh; patch management complying with configuration management documentation requirements. We perform preventative maintenance and ensure that the system is available consistently at 99.5%, above the metric requirement of 98%. We participate in evaluation of new network services and products; and we plan, design, implement tests and or deploy new products. Network management is essential to command and control practices and is generally carried out of a network operations center. Our approach covers:

Operation deals with keeping the network (and the services that the network provides) up and running smoothly. It includes monitoring the network to spot problems as soon as possible, ideally before users are affected.

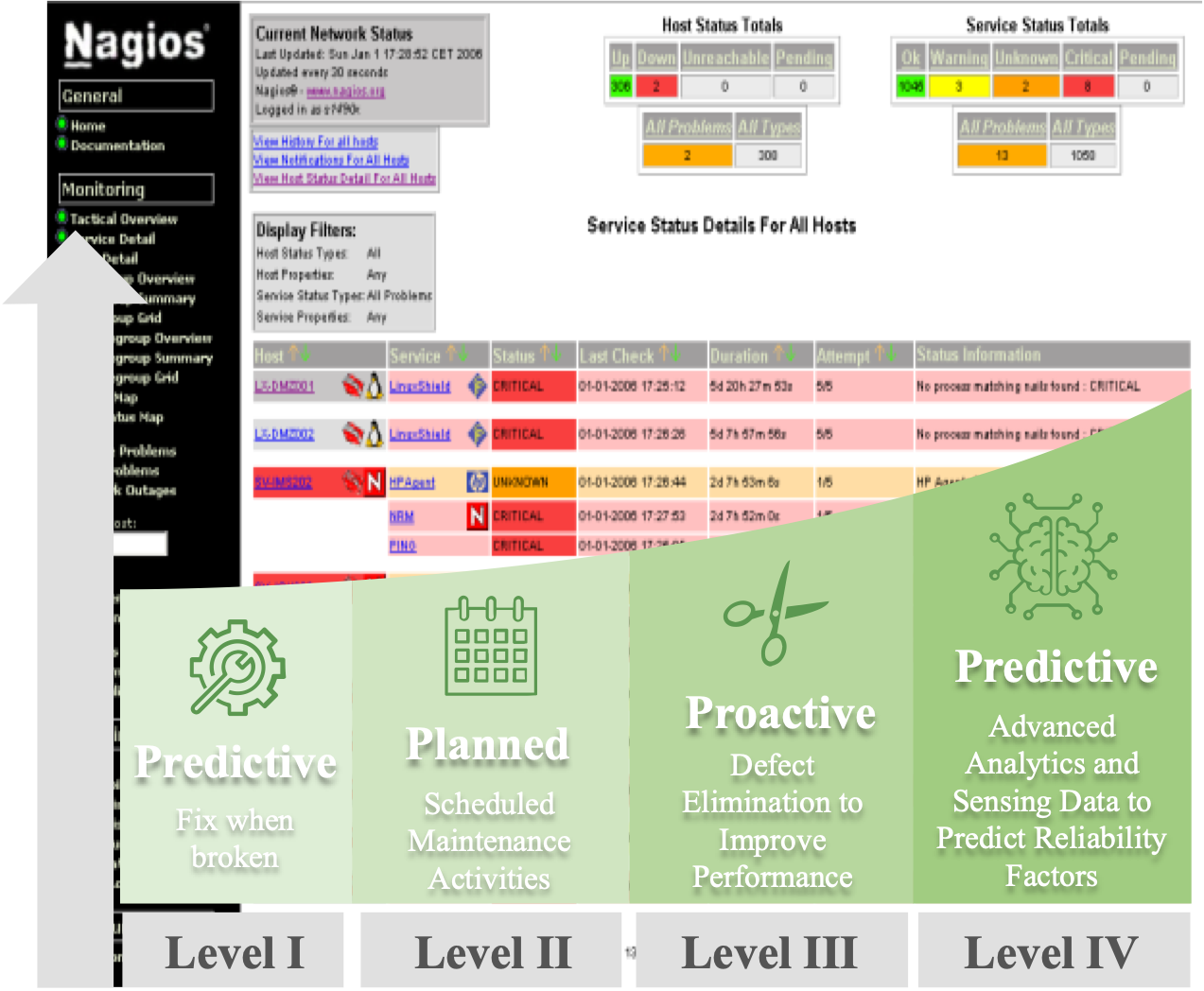
Administration deals with keeping track of resources in the network and how they are assigned. It includes all the "housekeeping" that is necessary to keep the network under control.

Maintenance is concerned with performing repairs and upgrades—for example, when equipment must be replaced, when a router needs a patch for an operating system image, when a new switch is added to a network. Maintenance also involves corrective and preventive measures to make the managed network run "better", such as adjusting device configuration parameters.

Provisioning is concerned with configuring resources in the network to support a given service. For example, this might include setting up the network so that a new customer can receive voice service.

A common way of characterizing network management functions is FCAPS—Fault, Configuration, Accounting, Performance and Security. The Hunatek team will provide network operations, event monitoring and management, performance monitoring, and analysis services. These services provide the capability for centralized operations, monitoring, management and analysis of network systems, core services, as well as network infrastructure assets to include trunks, circuits, routers, switches, cryptologic equipment, etc., 365 days a year, 24 hours per day, 7 days per week.

Services include, but are not limited to, monitoring established thresholds, responding to warning and alert messages from the monitoring systems, taking corrective action once thresholds are reached to prevent issues from occurring, and providing initial troubleshooting to restore services as quickly as possible. Other services include providing feeds to the Enterprise watch and other government designated watch centers as directed for situational awareness, responding to escalated incidents and outages (e.g., from the service desk), taking corrective actions to resolve the issue, escalating issues that cannot be resolved within the network operations center, and maintaining/upgrading the supporting network infrastructure and services.

Hunatek’s experts carry specific understanding, experience, and capability developing analytics, evaluating anomalies, producing analysis reports, and implementation of remediation and/or repair procedures to support cyber security. We have standardized methods to produce impact statements and cost analysis of anomalies in order to develop and implement remediation or repair actions. For Information Assurance (IA), our IA/cyber engineers research and respond to cyber security related TO requirements — for example, as contractors on the \_\_\_\_\_ contract, we assist with providing weekly summaries of new vulnerabilities, and, when available, related patch information. For assessments, we rely on our expertise with developing and updating Concept of Operations (CONOPS), Disaster Recovery (DR), and System Security Plans (SSP). The SSP is part of the Security Assessment Package (SAP) we will develop. Our staff has cyber security certifications – Computing Technology Industry Association (CompTIA) Security + CE certification. They also have certificates of completion for Operating System User Training in Linux and Windows OS/Server.

To ensure deliverables meet independent verification & validation (IV&V) criteria, we apply the processes laid out in the appropriate TO quality assurance criteria. We do IV&V, testing, code implementation, and document security as directed. We complete security testing and monitoring of all IT assets with network tools; providing reports on the results of testing and monitoring; identifying security levels and the type of data being handled; monitoring system activity; assigning and testing strength of passwords; and reviewing documentation to ensure compliance with all directives. The accompanying exhibit depicts our dashboard approach to proactive cyber information management. We supply staff with Tier 2 help desk experience. This includes customer-oriented service, tier 2 level technical expertise for a learning management system, system operations monitoring, collaboration with technical administrators to provide details, help desk metrics gathering and reporting.

## Other Task Areas

### 5.1. Functional Support

The contractor shall provide support services to the USAREC IT Projects, Programs, and Planning Division (P3MD). The contractor will support specific functional areas such as: requirements systems maintenance, sustainment, minor development, information management, business process modeling, enterprise architecture, data engineering, database management and administration, documentation, training, deploying software maintenance, integration engineering, process improvement, project management, and application software post-deployment support.

5.1.1. The contractor shall provide support services for IT sustainment.

5.1.2. The contractor shall support requirements development and sustainment for new and revised government applications and COTS application software supporting functional requirements.

5.1.3. The contractor shall deploy and sustain new and revised Government applications and COTS application software supporting functional requirements.

5.1.4. The contractor shall provide support services to the Government in the management and technical integration of externally developed products, modules, and/or applications into the existing architecture.

Hunatek understands it is critical to maintain business continuity through a robust support model. In providing services we support the primary objectives of for any outage providing normal service restoration as soon as possible, to minimize impact on the business and to maximize business value through upgrades to new functionalities. This focus will enable NIH users to operate in a supportive infrastructure where immediate support from respective technical teams is available when any errors or failures are encountered. Hunatek stands ready to perform as a government capable vendor, for all software and hardware component requirements, on a 24/7 basis, to address all IT Operations and Maintenance (O&M) issues encountered by users. Our team has experience with agency O&M infrastructure portfolios that include mainframes, client/server, web-based applications, and robust network architectures. Our planned support includes, but is not limited to: integration support, issue registration, issue remediation, and enhancements in the architectures, systems, and applications. We are able to support the objective of this task for the operation and maintenance of IT systems, keeping IT systems viable with supported vendor releases or off-the-shelf applications software upgrades.

Our Approach: For O&M efforts, Hunatek interacts with the customer and provides enhancements per customer requests. Software is constantly monitored during production and implementation. Help Desk support is provided to over \_\_\_\_\_ users across \_\_\_\_ agencies.

Solutions are delivered as Software as a Service (SAAS). All solutions are tested for scalability and growth. Hunatek utilizes the highest rated Security for Cloud delivering. There is basically infinite scalability available.

Operational Support: In order to provide Operational Support Network Monitoring, Control, Analyzation, and Performance Management functions are performed.

Software Maintenance and Upgrades: Software Maintenance and Upgrades include the functions Software Configuration Management, Software Engineering, Code Updates, New Releases, Modifications and Version Releases.

Telecommunications Maintenance (Data, Voice, Images, including Wireless): Telecommunications Maintenance is performed through VOIP configuration and installation and WiFi Configuration and Installation.

Infrastructure Management Services (IMS): Infrastructure Management Services require Network Management, Network Architecture, Policy and Configuration Management and Change Management.

Configuration Management: Configuration Management of systems includes CM Repositories, Change Management, Configuration Management Specialist, Administration Automation, Audit Procedures and Configuration Status Reporting.

Network/Hardware Support: Network Support services include Hardware Configuration and Installation, Network Troubleshooting, and Network Optimization.

Help Desk/IT Support: Included in IT Support are Helpdesk Specialists, Desktop Support, Mobile Devices Configuration and Support, End-user Support and Troubleshooting and diagnosing systems performance.

Resource Management: Resource Management services that are performed include the establishment of Performance goals and standards, Long-term planning, Mid-term planning and Short-term planning.

Backup and Recovery Management: Disaster Recovery Planning must consider Physical and Logical Backups and recovery systems.

Installation, Configuration, and Tuning: Typical Installations services performed are System configuration and Performance tuning.

Electronic Software Licensing Services including license: deployment, management, tracking, upgrading, etc: We utilize the approach of building a SAM team. We collect and manage inventory control across multiple platforms. Software installed is tracked and cloud based applications software as well. License entitlements are tracked.

System Management: These tasks are performed through integrated web based technology, progressive and innovative security and Data Center Maintenance.

IT Training: Customer training is critical to success. Onsite and CBT training with support are offered.

IT Operation and Maintenance Planning: Systems are constantly maintained and planning for maintenance improves the customer experience, optimizes effectiveness of operations and reduces technical and security risks.

Data Quality Management: Our data quality management is the management of people, processes, technology, and data within an enterprise, with the objective of improving the measures of Data Quality most important to the organization. The ultimate goal of our data quality management is not to improve the data quality for the sake of having high-quality data, but to achieve the desired business outcomes that rely upon high quality data.

Transformation Services: Our Transformation Services defines agendas and customer IT capabilities and operation to drive the business in a cost-effective and timely way. Functions include: IT operational model, IT governance and management, IT services delivery excellence, IT solution delivery excellence and IT workforce transformation.

Continual Service Improvement: The primary purpose of Continual Service Improvement (CSI) is to continually align and re-align IT services to the changing business needs by identifying and implementing improvements to IT services that support business processes.

* Review management information and trends to ensure that services are meeting agreed service levels
* Review management information and analyzed data trends to ensure that the output of ITSM processes are achieving the desired results.
* Conducting maturity assessments of process activities and roles to highlight areas of improvement or concern.
* Conducting internal audits verifying compliance.
* Conducting external and internal service reviews to identify CSI opportunities.
* Presenting recommendation to senior management for improvement.
* Leading managing and delivering cross functional and cross divisions improvement projects.
* Building effective relationships with the business and IT senior managers influencing all levels of management to ensure that service improvement activities are receiving the necessary support and are resourced sufficiently to implement solutions.

Balanced Scorecard for Operations: An operations plan design should outline the key strategy, priorities, areas of responsibility and critical performance measurements through responsible leadership and team performance toward measurable areas. Critical plan components include strategy, deliverables, performance indicators and organization. Key plan components include: Operating plan strategy; Deliverables; Performances indicators/measurements.

IT Infrastructure Optimization: Every organization can be at four different maturity level (Basic, Standardized, Rationalized or Dynamic). When we assessing the IT infrastructure optimization process, the below capability levels are reviewed at each maturity level: Identity and Access Management; Desktop, Device and Server Management; Security and Networking; Data Protection and Recovery; ITIL/COBIT based Management Process; Security Process.

### 5.3. Business Process Modeling

5.3.1. Develop, document, and integrate Business Process Models (BPM). BPMs shall be constructed with IAW Government guidelines and instructions. BPM work products and activities include:

5.3.1.1. Maintain version control of architecture products using approved version control processes.

5.3.1.2. Maintain compliance with BusinessEnterpriseArchitecture (BEA)5.0 or the current version.

5.3.1.3. Compliance with DOD and DA guidelines for business process modeling notation (BPMN).

5.3.2. Software requirements work products and activities include:

5.3.2.1. Development and maintenance of use cases.

5.3.2.2. Preparation and maintenance of user stories.

5.3.2.3. Trace ability between requirements.

5.3.2.4. Screen prototypes.

5.3.2.5. Identifying non-functional requirements for system service level and service level agreements, screen design, usability, and information architecture.

5.3.2.6. Maintain traceability from change request to requirement to software unit and version throughout the requirement. Must provide to the Government within 72 hours of completion.

5.3.3. Conduct formal Requirement Reviews for projects (an average of 150 projects over a five-year period). The Government functional representative(s) and the appointed representatives will be the approval authorities.

### 5.4. Software Engineering

Software development activities are limited to minor development incidental to systems maintenance and sustainment, which may include minor code construction, populating databases, integrating services, and other data files with data values; and other activities needed to implement the requirements and design. All activities must be presented to Government in the timeline set when acquiring the project. The Government, at its discretion and with approval of the Contracting Officer, may ask the contractor to follow an alternate development process or may waive some documentation requirements, particularly with minor change requests. The contractor shall: 5.4.1. Conduct software-engineering activities using applicable DoD and DA policies and standards, and industry best practices when applicable.

5.4.2. Perform minor software configuration, using requirements provided by functional and technical leads, including maintenance and sustainment of the architectural design and the detailed design.

5.4.3. Provide and store specific documentation and work products as defined by USAREC G6 software engineering methodologies.

5.4.4. Ensure developed products comply with appropriate and current Defense Information Security Agency DISA Security Technical Implementation Guides, including the Application and Security Development.

5.4.5. The contractor shall perform architectural design and the detailed design of each Configuration Item, as well as definition and recording of design decisions and descriptions. Documents shall be submitted to the Government within 24 hours of completion. Work products shall include designs and documentation such as:

5.4.5.1. Architectural designs, including identification of the software units comprising the CI, their interfaces, the integration between them, and the traceability between the software units and the Cl requirements.

5.4.5.2. Architectural design descriptions(e.g., interface software unit descriptions, interface descriptions, design descriptions, and database design descriptions).

5.4.5.3. Detailed design and description of each of the software units comprising a CI,(e.g., data manipulation, database access, and external and internal interfaces).

5.4.5.4. The contractor shall conduct formal design reviews by USAREC G6 methodologies.

5.4.6. Develop documentation for the software corresponding to each CI and the individual software units comprising the CI within 24 hours of meeting. All documents shall meet established guidelines within each project. All discretionary decisions will be made by the Government. The contractor shall draft documentation of such decisions. These documents include:

5.4.6.1. Project management plan.

5.4.6.2. Requirements documents.

5.4.6.3. Systems interface agreements

5.4.6.4. Memorandums of agreement.

5.4.6.5. Software installation work instructions.

5.4.6.6. Service Level Agreements.

5.4.6.7. Use case documents.

5.4.6.8. User stories.

5.4.6.9. Systems (and data) TransitionPlan.

5.4.6.10. Software Version Description.

5.4.6.11. Data Flow Diagrams.

5.4.7. Integrate software corresponding to two or more software units; test the resulting software to ensure that it works as intended. A report shall be given to the Government detailing test results.

5.4.8. Provide support services for the creation and maintenance of documentation for developer environments including: 5.4.8.1. Maintenance of standards and procedures for the developer environment

5.4.8.2. COTS material may be used where applicable, including Government acquisition of required updates and upgrades, as well as the material available for public use.

5.4.8.3. Documentation shall be in electronic format and indexed, providing rapid access to the information. 5.4.9. Create and maintain user and operations documentation including:

5.4.9.1. The development and maintenance of documentation for the users and operators of the system(s), updated and modified, as required, for the life of the system(s) or module user manuals, containing information needed by hands-on users of the software.

5.4.9.2. Quick reference materials, with system tips and reminders.

5.4.9.3. COTS material maybeusedwhereapplicable,includingGovernmentacquisitionofrequiredupdatesandupgrades, as well as the material available for public use.

5.4.9.4. Operationsdocumentationdevelopedforthesystem(s)thatmaybeupdatedandmodifiedasrequiredforthelifeof the system(s). Operations documentation work products may include computer operation manuals, which contain information needed to operate the computer software.

5.4.9.5. Documentationshallbeinelectronicformatandindexed,providingrapidaccesstotheinformation.

5.4.10. Provide all configuration items to the Configuration Management team within 72 hours of receipt of CI from the service provider.

5.4.11. Provide support services for software deployments to include, planning, preparation, and the fielding of software change packages, software components, and databases. The contractor shall plan and document software integration, installation, support activities, and training, including user, test-er, system administrator, and Customer Service Center personnel training.

5.4.12. Support or conduct a User Decision Meeting for each project before the deployment phase by established methodologies. The Government functional representative(s) or designated representative will act as the approval authority for the UDM.

5.4.13. Executable software shall specify all batch files, command files, services, media files, image files, script files, database files, data files, and/or other software type files needed to be installed or accessed to ensure successful operation of the software on the target configuration.

5.4.14. Prepare version descriptions that identify and describe the exact version of software prepared for each site. Work products shall include:

5.4.14.1. Software installation and integration plans.

5.4.14.2. Executable software and supporting documentation.

5.4.14.3. Software Version Descriptions.

5.4.15. Provide support services for other software deployment activities to include data migration, system deployment, and architecture component deployment. Work products include:

5.4.15.1. Fielding integration procedures, to include all aspects of data migration.

5.4.15.2. Automated installation procedures in support of the deployment of the systems software modules.

5.4.15.3. Architecture component deployment and fielding activities, such as site surveys (in coordination with the Communications, Electronics, and Operations MAM), and problem identification, isolation, and correction.

5.4.15.4. Training materials for users, Customer Support Center personnel, and supporting technical personnel before and during the deployment period.

5.4.16. Perform software lifecycle maintenance, as required, for any identified system or module. The contractor shall perform the same tasks described and update any plans and procedures that are impacted because of maintenance activities. A requirement for non-periodic software maintenance support shall be documented and communicated using a Request for Change.

5.4.17. Provide support services for operations by performing the following activities including:

5.4.17.1. Monitoring interfaces to ensure data is correctly sent and received with other modules and/or systems. 5.4.17.2. Monitoring production batch activities to ensure proper execution.

5.4.17.3. Resolving expeditiously any errors in production cycles to complete production activity.

5.4.17.4. Providing Level III and IV support to the customer to resolve production issues and/or guide customers and guidance training to support personnel. (Level III support refers to providing help with problems that are not resolved by the support and Level IV refers to requiring the assistance of a highly technical and knowledgeable software engineer or equivalent).

5.4.17.5. Within 30 minutes, assess identified reported system issues, failures and immediately initiate notifications and alerts through established procedures provided by the Government.

5.4.17.6. Identify and resolve problems in production systems.

Requirements Analysis: Requirements Analysis includes the following functions: Resolve conflicts between functional and performance requirements and constraints that arise during requirement analyses; Decompose functional requirements and allocate performance requirements during function analyses; Evaluate the effectiveness of alternative physical architectures and select the best solution during synthesis; Identify and analyze risk factors; Select appropriate risk handling approaches; and Manage risk factors.

System Design Alternative (SDA) Studies: The use of alternative studies is an integral part of the project process. Alternative studies use the defined scope to establish a validation design. Alternative studies are tailored to the intended application, inclusive of timing within the framework of the activity. Alternative studies are applied at all stages of the design process and may even be applied at the individual system or component levels. At the initial project level, the study should fully consider all life cycle cost impacts as input into making final decisions concerning which alternative to pursue.

The alternative study process is, at a minimum, a three-step process: (a) Delineate the deliverables or function and requirements that are required; (b) Identify alternatives that can meet the deliverables or function and requirements; and, (c) Evaluate and select one of the alternatives.

Systems Engineering: The primary goal of the system engineering process is to transform mission operational requirements or remediation requirements into system architecture, performance parameters, and design details. Beginning with the definition of a need, system engineering is a process that progress through the establishment of functions and requirements, performance of functional analyses, the identification and evaluation of alternatives, the solution of a preferred alternative, and validation of the preferred alternative. The process ends with verification that the need is met, including interfaces, fit, and completeness. The application of systems engineering to a project is tailored to the project’s needs.

Architecture Validation and Verification: Architecture validation and verification activities are conducted during the project life cycle to ensure that a project meets the defined mission by fulfilling the identified functions and requirements. Validation focuses strictly on the requirements and ensures the right problem has been defined. Verification focuses on the design solution for the validated requirements and ensures that the problem is solved. The formality and rigor of conducting and documenting validation and verification activities are commensurate with the associated risk, and the complexity of structures, systems and equipment.

Design Validation: The PM should validate that the developed requirements are complete and technically adequate with respect to the mission, and are consistent with each successively developed level of detailed requirements. This is done by assuring that requirements flow down from the facility to systems, to appropriate components, and finally to a task. Validation includes a completeness check of the system-to-system interface requirements, and ensures that these interface requirements link to appropriate interface control documentation where necessary.

Design Verification: The PM verifies that selected solutions meet validated requirements for high-risk structures, systems, and components. Verification methods that can be used include analysis, design reviews, system and component testing, and proof-of-principle demonstration testing. The rigor of verification performed is based on risk. Selected high-risk components could undergo several design reviews as well as testing to mitigate uncertainties associated with the identified risk. Also, proof-of-principle design demonstrations can be used for selected high-risk items where the test results help to define requirements and refine the final design.

Mission Analysis. Through a high level evaluation of project functions, provides sufficient information to develop more detailed functions and requirements during the conceptual and execution phases of the project.

Definition Phase. Takes the high-level function developed during pre-acquisition activities and uses functional allocation to determine functions to the system and subsystem level.

Execution Phase. Functional analysis is used to determine functions to the component level based on those developed for the system and subsystem levels during the Definition phase.

For complex projects, a database should be established to provide traceability of functions. The database should contain, at a minimum for all of the steps, the following information:

The functions, requirements, enabling assumptions and alternative evaluations by title including, for each, a description and a unique identifier.

The functions, requirements, enabling assumptions, and alternative evaluations cross-referenced with one another and with any interfacing functions or requirements; and

### 5.5. Applications and Web Integration

5.5.1. The contractor shall interact with service providers, other agencies, and vendors to ensure the efficient and effective operation of web applications. The contractor shall coordinate the interaction of operating systems, portal software infrastructure, COTS products, databases, and applications to ensure efficient application operation and an acceptable user experience. The Web integration support includes:

5.5.2. Advising and coordinating with developers, administrators, network personnel, and architects on changes to the architecture and technical environment.

5.5.3. Participating in the Virtual Architecture Team and assisting in developing and maintaining the USAREC, G6 Enterprise Technical Architecture documents.

Hunatek will develop customized software applications, database applications, and other solutions not available in off-the-shelf modular software applications. We employ many SDLC development methodologies, such as "traditional waterfall"; "Agile software development"; "rapid prototyping"; and "incremental". Hunatek's System Development Life Cycle framework provides a time tested sequence of activities for system designers and database developers to follow for software development. It consists of a set of steps in which each phase of the SDLC uses the results of the previous one. We try to adhere and follow SDLC lifecycle approach that is based on PMIs SDLC model and are well versed and skilled to deliver software development projects.

Scrum Methodology: Scrum is very well-known agile software development methodology. Scrum software development starts with the customer’s story. This story can be anything which a customer uses to describe their requirements. For instance, end-users need to add a new contact in address book, in order that he can interact with the person in the future by email postal mail. These stories are further explored by the software development team. In this scenario, the customer does not provide the full, thorough clarification of things and requirements that need to be completed in a project; however, the burden shifts on the shoulders of software development team for the reason that the software development team better understands how to solve the problem they are provided with. Hence, in the Scrum software development a sprint planning meeting involves the discussion on the required results. In the Scrum methodology, the software development process is measured through a series of sprints. Normally, these sprints are delivered within a duration of two weeks. In this scenario, a meeting is conducted in the beginning of each sprint, in which project team determines what requirements they can complete, and then develop a sprint backlog on the basis of this analysis as well as a list of the actions needs to be carried out during the sprint.

Production Deployment: Creating applications in four steps

Development: Optional. This is the working environment for individual developers or small teams. Working in isolation with the rest of the tiers, the developer(s) can try radical changes to the code without adversely affecting the rest of the development team.

Integration: A common environment where all developers commit code changes. The goal of this environment is to combine and validate the work of the entire project team so it can be tested before being promoted to the Staging Environment. It is possible for Development and Integration to be the same environment (as in the case where the developer does not use a local copy of the source code).

Staging: The staging tier is an environment that is as identical to the production environment as possible. The purpose of the Staging environment is to simulate as much of the Production environment as possible. The Staging environment can also double as a Demonstration/Training environment.

Production: The production tier can include a single machine or a cluster comprising many machines.

Application Prototyping: Following is the stepwise approach to design a software prototype:

Basis Requirement Identification: This step involves understanding the very basics product requirements especially in terms of user interface. The more intricate details of the internal design and external aspects like performance and security can be ignored at this stage.

Developing the Initial Prototype: The initial Prototype is developed in this stage, where the very basic requirements are showcased and user interfaces are provided. These features may not exactly work in the same manner internally in the actual software developed and the workarounds are used to give the same look and feel to the customer in the prototype developed.

Review of the Prototype: The prototype developed is then presented to the customer and the other important stakeholders in the project. The feedback is collected in an organized manner and used to further enhancements in the product under development.

Revise and enhance the Prototype: The feedback and the review comments are discussed during this stage and some negotiations happen with the customer based on factors like, time and budget constraints and technical feasibility of actual implementation. The changes accepted are again incorporated in the new Prototype developed and the cycle repeats until customer expectations are met.

Multimedia Software for Patient/Staff Education: Through the use of CBT online, educational content can be delivered directly to patient and staff through online portal. Content can be pushed using a content management system and the utilization of CBT web base training software. This approach helps to cut down on overall cost of media delivery. Along with CBT online portals, the ability to develop mobile app that runs on most mobile devices is an alternative for training content to be delivered directly at the user’s finger tips.

Program Evaluation Software: Because it takes more than just software for program evaluation for the tracking and analyzing of data in order to make any meaningful conclusions. We treat program evaluation within a full project lifecycle. Our team work through the defining of the customer’s evaluation process, track constituent data and outcome, track non-constituent data, analyze and display measures. Each one of these phases will help determine the best program evaluation software that best fit the needs of our customer.

Business Intelligence and Analytics: Big Data is the technology that stores and processes data from sources both internal and external to one’s business. The use of the Big Data technology which makes available almost limitless amounts of information one can sift through for insights related to their specific industry such as healthcare. Business Intelligence goes beyond the data to include what business leaders actually do with the insights they glean from it. It involves the processes and procedures that support data collection, sharing, and reporting. The analytics from which are drawn by slicing the data based on process and procedures can help the end—user make better informed decisions. Our team will help define the processes and procedures taken from existing workflows to define what kind of key performance indicators are to be generated and reported.

Web 2.0 Development and Management: Our team builds web-based communities, hosted services, and applications that facilitate communication, information sharing, interoperability, and collaboration. Our belief with Web 2.0 development is to allow users to do more than just retrieve information. WE build complex software-applications that run entirely through a browser. Our Web 2.0 design uses rich, user-friendly interface based on Ajax and similar client-side interactivity frameworks, or full client-server application frameworks such as Flex.

Hunatek is committed to making our deliverables and any work products compliant with the accessibility standards of Section 508 (Electronic and Information Technology (EIT) Accessibility Standards, 36 C.F.R. § 1194). Hunatek employs a Section 508 compliance standard operating procedure (SOP), which includes instructions on: staying current, adjusting audit tools, and conducting a formal training program to create Section 508 awareness and adoption of best practices. We strive to comply with the applicable standards of Section 508 of the Rehabilitation Act to the maximum extent possible, ensuring that individuals with disabilities have comparable access to and use of information and data to that provided to the general public, unless an undue burden would be imposed on us.

### 5.6. Data Engineering

The contractor shall develop, document, engineer, and integrate logical data models and physical data models in support of a task. Data models shall be constructed daily by Government guidelines and instructions to ensure that developed models are reflected in the Government data engineering processes. Data modeling work products and activities shall include:

5.6.1. Logical Data Models, Physical Data Models, and Entity Relationship Diagrams including those that conform to DOD standards such as the DOD Enterprise Data Model Standards outlined in the DoDAF.

5.6.2. Logical Data Model documentation shall be developed using Computer Assisted Software Engineering tools.

Database Development and Management: Our team takes data in any format and output a standardized and formatted database that is ready to use. Our data management process covers expertise in various functions such as:

Data Warehousing: Uniform data and format structure with ETL

Data Processing: Migration, Standardization, MIS, Communication

Data Capturing: Manual, Automated (Scanning)

Multi point Data Management: Web/Internet based multipoint access, upload, amendment authority, and administrative/usage rights

Application Support: Requirement analysis, application design, solution mapping, application development, implementation

Integration: Data and Communication integration for multipoint information processing, tracking and action standards.

### 5.7. Database Management and Administration

5.7.1. Provide support services for Government enterprise databases in development, test, and production environments. This support shall include, but is not limited to:

5.7.1.2. The analysis, transition, and mappingoflegacydataandexternalsystems'data,toincludeidentificationofdata sources, mappings to the automation systems, LDM, and the physical database design, and support for subsequent mapping of the physical data to systems databases.

5.7.1.3. The maintenance of the Production and DataWarehouseDataDictionaries,ensuringthattheyfollowtheDODData Standards.

5.7.1.4. Creationofperiodicupdatepackagesofstandardizeddataelementsandsubmissionofthosepackagestodesignated Government approval authorities for review and implementation.

5.7.1.5. Conductingperiodicdatabasemaintenance(daily,weekly,andmonthly).Maintenanceactivitiesshallbeconducted at times approved by the government and that have minimal impact on the organizational mission.

5.7.1.6. Continualmonitoringandoptimizingoftheproductiondatabaseenvironmentsinconjunctionwithhostservices, including maximizing system performance within the application, maintainability, and reliability.

5.7.1.7. Maintenanceofcontingencyplanstoupholdestablishedservicelevels,executionofbackupsinsupportoftheplan, and execution of recovery of all database components as required.

5.7.2. Perform a set of regular tasks in support of software applications and related servers that includes the operation and maintenance of Government provided COTS and custom-developed application services and software. Tasks shall include:

5.7.2.1. TheinstallationandmanagementofCOTSserver-levelsoftwaretoincludetoMSProject®,SharePoint®,Centra VCS®, SUN ON'E Portal®, Documentum ®, LDAP ®, ePiphany®, Web Trends ®, SumTotal Systems®, e-ROOM ®.

5.7.2.2. TheinstallationandmanagementofServiceOrientedArchitecturegovernance,security,andmanagementtools including System and Layer7.

5.7.2.3. Supportforthemanagementandtechnicalintegrationofexternallydevelopedapplicationsandmodules,and updates thereto, into the enterprise architecture, to include a review of plans, coordination of project milestone events, integration of the item into the appropriate technical layer(s) (including database layer), validation, and deployment.

5.7.2.4. Supportcustom-codedapplications,someofwhichconnecttointernalandexternaldatasourcesonmyriad platforms and from a variety of database systems.

5.7.2.5. Implementingsecurityandsoftwareupgradepatches. 5.7.2.6. Supportforscheduledmaintenanceperiods.

5.7.2.7. Receivingandrespondingtotroubleticketsforenterprisearchitecturekeybusinessandinfrastructureapplications incidents.

### 5.8. Project Management

The contractor shall provide effective management of project schedule, performance, risks, subcontracts, and related data. The contractor shall follow a Government approved project management process that offers:

5.8.1. Integrated Master Schedule, with clear milestones, which provides accurate and timely schedule and performance information throughout the life cycle of the program.

5.8.2. The conduct of project milestone reviews using a government template.

5.8.3. Risk management to mitigate program and/or project risks and provides for special emphasis on software development efforts through the integration of metrics to monitor program status.

5.8.4. Active participation by contractor's senior management in project administration and problem-solving. 5.8.5. Communications and change management processes that involve all key stakeholders.

5.8.6. Documented procedure for estimating costs and schedules to ensure consistency.

5.8.7. Providing project status reports to the Government on a weekly basis or as deemed needed.

Hunatek demonstrates specific understanding, experience, and capability managing acquisition systems as part of our Project Management capabilities. From years of service to the DOD, we understand systems development using the Joint Capabilities Integration and Development System (JCIDS) IT Box Model and acquisition management in accordance with DoDD 5000.01 and DoDI 5000.02. Hunatek systems engineers have implemented the IT Box model using fewer iterations of validating documents through the JCIDS process. This is accomplished by describing the overall IS program in the IS ICD, and delegating validation of detailed follow-on requirement and solution oversight to a flag-level organization.

Hunatek applies a robust formal and informal communications framework to share information gathered from weekly or monthly meetings with the client Program Manager, periodic status meetings, formal Program Management Reviews (PMR), and day-to-day interactions. For our clients, we will create the comprehensive Master Project Management Plan with subordinate Risk Management Plan, Human Resource Plan, Communications Plan and Quality Plan for each project. We have provided these artifacts on many of our engagements, such as our previous \_\_\_\_ and \_\_\_\_\_\_\_\_ projects. This framework has led to high client satisfaction on past and current engagements.

In alignment with our CMMI Level 3 processes, Hunatek will prepare and provide weekly updates of our integrated schedule, risks, action item logs, and plans. These status reports allow clients, Hunatek managers and executives to stay fully abreast of project activities, ensuring service and deliverables are meeting quality standards.

Hunatek is a quality-driven organization that incorporates principles from ISO 9001 and key tenants of CMMI. In order to maximize timely responsiveness to our clients, Hunatek delegates decision-making authority to the on-site Project Managers. The Project Managers will have authority to act and make decisions binding Hunatek on all technical matters. Our Chief Operations Officer serves as a trusted resource to ensure quality and timely delivery for all contract deliverables and provides our Project Managers with access to comprehensive corporate resources to assist them, including a Quality Control Manager (QCM), all provided at no additional cost. The QCM will assist the Project Managers with ensuring performance meets or exceeds our quality performance standards.

Hunatek utilizes a suite of applications for time tracking, contract adherence, task order management for subs, invoicing, and Earned Value Management (EVM). This last tool helps our PMs to measure project performance. It is a systematic project management process used to find variances in projects based on the comparison of worked performed and work planned. EVM is used on the cost and schedule control and can be very useful in project forecasting.

Hunatek utilizes Deltek’s accounting system in conjunction with our own ISO-certified processes. Deltek's industry-leading Project & Portfolio Management (PPM) solution provides effective cost management, scalable scheduling and reliable risk evaluation. This system provides an EVM module that enables the use of program controls best practices — which provides us the ability to quickly produce accurate, detailed reports so our team can then spend more time analyzing project performance and applying corrective actions.

Our accounting solution, certified by the Defense Contract Audit Agency (DCAA), is integrated with MS Project, and fully integrated with our General Ledger, Payroll, and Human Resource (HR) functions. Hunatek requires all subcontractors to record time and manage travel in our enterprise resource planning system (ERP). This technique allows our team to have near real time insight into the fiscal and human capital well-being of the project. Likewise, each subcontractor monitors their workforce without delays.

### 5.10. Software Integration Engineering

The contractor shall provide Software Integration Engineering support to coordinate the technical architecture and the integration between major components thereof. 5.10.1. Overseeing the applications systems architecture and collaborating with development teams, operations staff, and external engineers to ensure systems security compliance, efficiency, integrity, and maximum operational availability within the overall enterprise architecture.

5.10.2. Providing advice and coordination concerning technology insertions into the enterprise architecture. 5.10.3. Creating technical and system views and models by the DODAF.

5.10.4. Assisting in the sustainment of the enterprise architecture technical architecture and its related documentation (in coordination with other technical staff).

5.10.5. Reviewing project scope documents, requirements, procedures, processes design and plans to determine the technical impact on other areas, systems, sub-systems, and modules of the enterprise architecture.

5.10.6. Providing support services to the Government's Virtual Architecture Team, which works to integrate technical projects into the overall architecture by reviewing project technical design plans, to accomplish the following: conduct rapid technical assessments and implementation impacts on selected products and projects; provide support to resolve cross-system / sub-system / module problem identification and resolution; analyze technical infrastructure issues; support the maintenance of technical architecture documentation, diagrams, and views; and support the Government's strategic long-range technical efforts.

Hunatek’s IT support services provides a complete end-to-end solution for agencies, including software deployment, maintenance, monitoring, backups and system support. The IT Services delivers transparent services to the federal community, which provides the highest degree of reliability, accountability, and security while maintaining cost effectiveness and agility. An integral part of these IT support services is also pro-actively conducting security scans and applying security patches to prevent any unauthorized access of the data, performing database tuning to makes sure accessibility and user experience is not negatively impacted while running simple to complex queries on production database environments.

Our Application Support model is an evolved and proven multi-tiered framework on which our support solutions are based upon that are offered to suit all needs of our customers. Our support model provides high-availability service products in a networked environment. In the leveled support model, organizational functions are placed in an escalation hierarchy with clear lines of demarcation between functions to ensure that responsibilities and duties are clearly defined. Depending on the nature of the IT infrastructure, how many users there are, and how critical it is to the agency’s day to day operations, we tailor a solution to meet those exact needs. We have a record of providing staff that are ITIL certified and have sound knowledge of IT Service Management (ITSM) best practices. Our approach is in complete alignment and compliance with ITIL methodology for support and maintenance for infrastructure. The following key components of this methodology are:

Incident Management – Hunatek is well-versed in the use of support desk ticket management tools, such as ‘BMC Remedy’ to enable tracking and management of all government user issues. In use of these tools, unplanned interruptions to IT service will be characterized as an “Incident” and shall be restored through Incident Management Processes defined in applicable Service Level Agreements (SLAs). Users will report incidents to the Help Desk, a ticket shall be created by Help desk personnel, and the incident shall be handled in accordance with guidance specified in the appropriate SLA. These SLAs are a critical component for providing customer service to government, and shall be rigorously followed throughout the support and maintenance process. Trouble tickets shall be prioritized and corrected, based on urgency parameters and associated timelines specified in the SLA. For instance: Priority 1 tickets may have resolution requirements of within 20 minutes.

Problem Management – Undetermined root cause of one or more incidents is defined as a ‘Problem’. Hunatek shall take proactive action to resolve problems as quickly as possible, and take the appropriate action required to prevent reoccurrence. Our team shall store all problem related information in a centralized database, and use state-of-art technology to analyze the data, search for obvious and non-obvious relationships, use that information to perform a root cause analysis and identify fixes.

Change Management – Enhancements to the existing architecture shall be prioritized, based upon business urgency and associated rules specified in government Change Management SLAs supported by Hunatek All change requests shall be submitted by the user community, to the Hunatek Change Management staff, who shall comply with all change management procedures specified in the Change Management SLA. Once approved, changes shall be implemented using methodologies, processes and tools specified in the that SLA. The goal is to maximize the business value, with minimal impact to business operations.

Release Management – The components required to implement one or more approved change requests is known as a ‘Release”. Hunatek recommends that all government release management processes be aligned to ITIL, and documented in a Release Management SLA. The goal is to develop comprehensive deployment plans that ensure release can be built, tested and deployed efficiently to minimize impact production services, associated with government operations.

Information Systems Security: Ensure the confidentiality, integrity, and availability of our IT systems. Ensure systems capable in the areas of information systems security, network security, and security analysis. Conduct in-depth technical reviews and validation of all new and existing IT systems to identify potential security problem areas before they arise.

Security Operations Center Development and Operations Management: Provide a variety of security operations center development and operations services: security policies, procedures, and guidance requirements, analysis, and modeling; firewall design, implementation, and management; and infrastructure design and security training. All transactions and attempted transactions are audited in real time with reporting to the operation center. Provide customized dashboards for viewing security operations status.

Application Security: Develop defense-in-depth security architecture for protection against cyber threats using content and application security solutions. Invoke levels of testing to determine whether the application is vulnerable to common or unique attacks (such as attacks on application logic). Use penetration testing to simulate the types of attacks, including those that attempt to subvert the application's unique security mechanisms.

Disaster Recovery: Provide support in preparing IT contingency and disaster recovery plans in accordance with federal guidance and NIST Special Publication 800-34, IT Contingency Planning Guide for Information Technology Systems. Create contingency and disaster recovery plans and conduct testing on a regular basis. Provide architecture that enables redundancy running in secure FEDRAMP cloud environment.

### 5.11. Training Support Services for Recruiting and Retention College

5.11.1. Technical Support Analyst. Contract Technical Support Analyst(s) are required to up-load tests, lesson plans, and training data into Blackboard and Training Development Capabilities. The Government will ensure the Technical Analyst(s) has access to all required equipment and resources to perform all training development functions to approved standards of the Government. The contractor shall ensure the Technical Analyst(s) execute training activities and functions by the established timeline. The Technical Support Analyst(s) is required via blackboard to make announcements for all users, announcements for instructors (Cadre) only, disseminate new lesson plans, ideas, and courseware, provide Bulletin board capability with threaded discussion topics, provide the conferencing capability for instructor-facilitated classroom discussion, provide chat room capability to process other training support activities as necessary. The requirements for TDC will require CAD, LP, ITP, CMP, SEP, Test, and PE.

5.11.2. Training Analyst. Training Analyst(s) are required to develop, write, and review documents, plans, and or reports for assigned topics or courses within USAREC. The government will ensure that the Training Analyst(s) have access to all required equipment and resources to perform all training development functions to the approved standards of the Government. The Contractor shall ensure the Training Analyst(s) produce the deliverables by the established timeline. The requirements for TDC will be CAD, LP, ITP, CMP, SEP, Test, and PE.

5.11.3. The Technical Support and Training Analyst(s) shall go through an orientation period to learn the RRC organization. The Training Analyst(s) shall become familiar with the target audience of the respective course and review the Program of Instruction (POI). It shall also include familiarization with the respective lesson plan from which the instructors present in the classroom instruction. This period shall be from 30-60 days after recruitment and reception at RRC.

5.11.4. The Technical Support and Training Analyst(s) shall attend meetings, conferences, briefings, and other information- sharing venues when necessary to perform specified tasks under the contract.

5.11.5. The contract Technical Support and Training Analyst(s) shall remain current on Army doctrine, regulations, and other policy and procedural changes.

5.11.6. The Technical Support and Training Analyst(s) shall meet with Subject Matter Experts (SME) and Course Manager to draft lesson plans generated from task analyses on assigned courses in TE 4, and shall play a key role in

determining the sequence and order of lesson plans, and the incorporation of applicable technology and design. The contractor shall submit all lesson plans to the COR or designated Government representative for review and approval.

5.11.7. Helpdesk technician to provide troubleshooting, account management, software updating, and imaging computer systems.

At Hunatek, we believe client education and training is a subsystem of an organization’s ITIL-based process improvement, because it ensures inconsistency is reduced, and learning or behavioral changes take place in a structured, repeatable format. Our team regularly uses SharePoint site as an education portal for our employees and government personnel as necessary. We have created specialized MS Office training for our other customers and update lesson plans, education curricula and personnel training requirements for all key personnel. Whether Standard Operating Procedures (SOPs), processes, key IT initiatives or security, our team provides a mechanism for personnel growth through computer based training (CBT), teach the teacher or on-site, instructor based training. We strive to stay ahead of the curve for preparing personnel for their responsibilities and updating them as they progress. The following model will be used to provide the training necessary:

Training will be developed for all staff as needed. This will include general awareness training modules as well as system-specific or role-based trainings that are more detailed and likely pertain only to a subset of the entire staff.

Appropriate methods of training as they pertain to the subjects of the training are: Webinar or slideshow format may be appropriate for general training; Instructor-led training session may be appropriate for system manipulation or database security and privacy training; Training programs will be periodically evaluated for effectiveness; and, Training programs will also be evaluated regularly for currency, as technology and the privacy and security fields are constantly changing.

Distributed Learning Innovation: Although classroom training is still used by many agencies, the move in the training community is toward DL, also known as blended learning, for delivering training to adult learners. We will use DL in combination with the best of classroom training and Computer Based Training (CBT) and Web based Training (WBT). Reducing the amount of classroom training hours reduces costs and increasing the amount of CBT and WBT reduces costs and enables the development of more comprehensive critical thinking skills through the use of simulations.

Section 508 accessibility standards are routinely implemented by the courseware developer and our understanding of Section 508 Compliance is enhanced by our active participation with the W3C Web Accessibility Initiative Working Group. WBT will carry a mobile-device friendly interface, so that training participants may avail themselves of study in many environments.

### 5.12. Process Improvement

The contractor shall provide process improvement using industry best-practices. The contractor shall provide process improvement using industry best-practices. The contractor shall conduct Process Improvement activities including following tasks:

5.12.1. Provide support services to the activities of the organization's Process Action Teams, Software Engineering Process Group, and the Government's software process oversight committee.

5.12.2. Create and maintain the process improvement plan to consolidate in a single document the planning information to systematically improve the organization's process maturity.

5.12.3. Facilitate the creation and/or maintenance of organizational process improvement documentation.

5.12.4. Develop, update, and/or provide appropriate training material to support the training of the processes.

5.12.5. Provide support services in process improvement assessments, including on the organization’s Project Management Methodology and related processes, as required, or when requested.

### 5.13. Information Technology Asset Coordinator

The contractor shall provide the asset coordinator:

5.13.1. Responsible for administrative duties within the IT procurement and inventory management function.

5.13.2. Maintains records and databases containing information regarding licenses, warranties, and service agreements for the organization's hardware and software.

5.13.3. Responsible for documenting and tracking IT assets after delivery to ensure all equipment and software are accounted for.

### 5.14. Telecommunications Control Officer

5.14.1. Process all communications requests within the command to include installation, removal, transfers, and resolving customer inquiries.

5.14.2. Track and monitor various telecommunications services including local and wide area networks, voice mail systems, wireless and digital services, peripheral equipment, offline message preparation equipment, and telephone switch modernization.

5.14.3. Review actions are completed, and a thorough record is maintained to aid in the validation of billed services. 5.14.4. Perform technical reviews.

5.14.5. Compile support documents and reports, identifies, and notify users of problems, and maintain usage reports. 5.14.6. Provide user training and develops procedures and efficient systems operation.

5.14.7. Review and assist to ensure landlines, smartphones, and tablet data transmissions are properly controlled and use the most economical communications means available.

5.14.8. Contact telecommunication carriers, vendors, or communications representatives to obtain estimated costs for requested services including requests for service, coordinating dates of service, and resolving billing problems.

5.14.9. Manage telecommunications program for USAREC.

5.14.10. Provide technical and managerial guidance for communications.

5.14.11. Research, plan and implement new or upgrades to existing telecommunications and/or data communications systems.

5.14.12. Process requests for new telecommunications and or data communications systems.

5.14.13. Obtain clearance to add and delete data in JRMS and GSA Tops Government systems.

5.14.14. Resolve telecommunications incidents, trouble tickets, and requests for information.

### 5.15. Test and Evaluation

The contractor shall provide testing and evaluation:

5.15.1. Types of testing may include:

5.15.1.1. New and existing baseline images and releases

5.15.1.2. New and existing operational releases

5.15.1.3. New and existing GOTS and COTS applications

5.15.1.4. Access methods and associated security

5.15.1.5. Application security testing

5.15.1.6. Technology projects

5.15.1.7. Hardware configurations (i.e., printers, scanners, and other supportive devices)

5.15.2. The contractor shall perform a set of regular tasks in support of the application administrations that includes the operation and maintenance of the government-provided test and evaluation toolsets and related hardware. Tasks shall include:

5.15.2.1. Customize/code application modules and data fields to support metric collections and processes improvement. 5.15.2.2. Implement security and software upgrade patches.

5.15.2.3. Provide validation of test toolsets as required.

5.15.2.4. Receive and respond to trouble tickets for the testing toolset within 24 hours.

5.15.2.5. Coordinate formal requirements, delivery, and administration of the enterprise test and evaluation toolset. 5.15.2.6. Design, maintain and administer the centralized and secure repository.

5.15.2.7. Collaborate with system administrators and vendors to ensure operations of the testing toolset.

5.15.2.8. Participate in the configuration and testing of test toolset changes.

Hunatek will gain a final customer acceptance signature (attestation) upon successful completion of each application after final satisfactory user acceptance; and final client (RD QA) acceptance. This follows successful completion of Deployment Readiness Testing (DRT) performed by the government. For delivery, after acceptance testing has been signed off by the government, the system will be cleared for deployment. Of course, prior to acceptance, we undertake a full suit of testing and evaluation.

Unit testing is conducted on each new or modified unit of code produced by the software development team. This applies to both application source code and database source code. During initial development, unit tests are conducted on groups of code that comprise a Test Point. In addition, during the testing phase, a unit test is conducted on each fix, which has been developed to correct a Software Trouble Report. The source code is unit tested by the developing programmer before it is submitted for peer review. These unit test phases are also known as Arrange, Act and Assert, or simply AAA. We will implement static testing, conducting “walkthroughs” and reviews of the design and coded components. We will offer secure code reviews; if it is not accomplished in the development phase, we will ensure it is completed in the beginning of the testing phase. We will check for executing path testing based on normal flow, on decision points, and on examining the assignment and use of variables in a (data flow) program. Finally, unit testing will address checking the validity of loop constructs and executing unexpected error conditions.

Hunatek will provide functional testing to verify by checking an application against design documents and/or specifications. We will write test plans and test cases. Hunatek’s functional testing starts with the identification of functions that the software is expected to perform. Then we check the creation of input data based on the function's specifications. We make the determination of output based on the function's specifications and the execution of the test case. we then make the comparison of actual and expected outputs. Hunatek’s functional testing will focus on requirements for testing that can be traced directly to use cases, business functions and rules. Our goal of this testing is to verify proper data acceptance, navigation, processing, retrieval and the appropriate implementation of the business rules. Our technique includes executing each use case, use case flow, or function using normal course of event and alternate flows.

Hunatek will test the fixed defects by making sure the problem identified in the defect is corrected and did not create any adverse impact to existing functionality. If required, additional tests might be created to test the defect fix and those tests will be incorporated into functional and regression test suite. Any defects identified during different testing types will be logged into JIRA tool. Hunatek QA lead will participate in change control board (CCB) meetings to review the defect severity and coordinate with development team to fix all the blocker, critical and major defects identified during testing and we will make sure those defects are retested and fixed before the production deployment. We will follow the Defect Severity Definitions outlined in the PWS.

Hunatek’s objective of regression test is to ensure that changes or enhancements have not introduced new defects in the current or previous iterations. As the function of a software application grows with each succeeding release, so do the regression testing needs. To manage this, Hunatek will use Automated Intelligent Regression Testing (AIRT), which intelligently runs automated regression suite relevant to the changes in code. We can reduce the overall regression test cycle by identifying and executing only the set of scripts to satisfy the test scope. Hunatek will also use exploratory testing skills as part of regression to catch defects that automated scrips might miss.

Hunatek SME at RD was responsible for researching, recommending, and implementing tools to increase automation on the project. We proactively introduced innovative automated testing strategies and toolsets into the overall RD development processes. This process became part of continuous integration (CI) and continuous delivery (CD), especially when it comes to regression testing.

Hunatek will perform smoke testing to determine if a new software version is installed, configured correctly, and stable enough to accept for a major testing effort. If the application is unable to pass the smoke test, the build is returned for correction. As part of smoke test, Hunatek will verify whether the important features are working and there are no blockers in the build that is under testing. If our smoke test suite fails, build is declared as unstable and the build or application is returned for correction.

Hunatek will perform security testing, which is essential for software that processes sensitive and confidential data to prevent system intrusion by malicious users. Security testing of the system controls will determine the extent to which the security controls in the information system are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security requirements for the system. We will perform stage gate security reviews to identify security vulnerabilities in application/system architecture/design, implementation, and deployment, according to RD security policies and standards. The reviews will include security design review, security code review, and vulnerability scan. We will check for compliance with steps 1-3 of the USDA Six Step Risk Management Framework (RMF) in order to begin assessing the security controls for the applications.

Our team will work with the RD Security and the Privacy A&A team to perform an A&A of the system. Accreditation Process (also known as A&A) is the result of an independent system test and evaluation (ST&E) performed by a third-party assessor. Once HIGH and Critical vulnerabilities are remediated, MEDIUM and LOW defects/vulnerabilities may be addressed in a POA&M report. If the Department concurs with the findings in the accreditation package, the application/system will receive an Authorization Letter for Authority to Operate (ATO) on the USDA / RD network. Hunatek will setup, configure, deploy, and maintain all agency specific dynamic and Static analysis tools used in the security testing and verification process. All Scanning tools including but are not limited to: Dynamic Tools: HP Web lnspect; IBM AppScan; IBM AppScan Enterprise; Burp Proxy; Zed Proxy. Static Analysis tool: Checkmarx; IBM AppScan Source; SonarQube. Reporting: Threadfix; JIRA.

We will: Perform vulnerability scan and/or penetration testing for RD applications, services and databases to identify risk and Issues using the relevant methodologies: automated and manual approaches. We shall follow the industry standards like The Open Web Application Security Project (OWASP) top 10 for 2017 and 2013. The scanning efforts are focused on potential risk areas identified in earlier stages, and appropriate tools and techniques are utilized accordingly. Also, report all identified issues along with their initial technical risk evaluation on issues that may require immediate attention.

The results of Hunatek security tests are compiled into a report detailing specific vulnerabilities that were exploited, what sensitive data that was accessed, and the amount of time the pen tester was able to remain in the system undetected. This information is analyzed by security personnel to help configure the USDA RD enterprise settings and other application security solutions to patch vulnerabilities and protect against future attacks. We deliver reports quickly, within ten business days of finalizing the security test.

Acceptance Testing in a government provided environment similar to production is the most critical phase in the software development lifecycle. Hunatek will submit test scenarios (user stories) and test cases for government acceptance. All test cases and scenarios will trace to the requirements and design documents signed off in phase two and three (via a Requirements Traceability Matrix document)closely work with RD QA team to successfully execute the acceptance testing by providing support in setting up tools for test data, defect management, test scenarios and test cases. Hunatek will also perform regression testing of defects found during acceptance testing.

Evaluation and Prioritization: Full study of interoperable standards led to full performance specifications.

Detailed Requirements: Reviewed with DOD and finalized specifications.

Design and Analysis: All coding was developed based upon standards.

Implementation and Developer Testing: Systems testing and simulation was confirmed with standardized testing. All systems and modules passed testing.

QA/Acceptance Testing: Systems testing to certification standards was performed. Testing completed and all systems met certification requirements.

### 5.17 General System Support

The contractor shall:

5.17.1. Perform WebLogic administration and multi-server management.

5.17.2. Provide technical training materials and seek mentoring opportunities to promote growth and increase competency.

5.17.3. Work requires experience with DAC, Informatica 7. x, 8. x.

5.17.4. Promote team creativity and cohesiveness to ensure that technical designs fit into the overall data warehouse architecture and to facilitate fairness while striving for consensus in problem-solving.

5.17.5. Metadata and Content Management.

5.17.5.1. Collaborate with DBAs, Data Integration, Metadata, and BI Delivery Team to address BI Project needs

5.17.5.2. Devise & analyze BI Metadata/Logical Data Model in a graphics chart

5.17.5.3. Translate BI requirements into analytics metadata Devise & Test Metadata

5.17.5.4. Collaborate with IT BI SMEs to define high-level report/analysis, iBots/alerts, and overall intelligence dashboard functionality and user experience

5.17.5.5. Design & Build BI Delivery components (Dashboards, Reports, BI Publisher bigots, etc.)

5.17.5.6. Perform performance tuning as it regards OBIEE reports (i.e., where are calculations performed, etc.) 5.17.6. Defining Requirements and Customer Technical Support.

5.17.6.1. Coordinate interactions with customers and business analysts to establish common business information requirements, analyze data to satisfy those requirements, and execute specific technical solutions to achieve stated business goals

5.17.6.2. Strive to exceed customer expectations in the delivery of BI solutions for dashboards, BI Publisher reports, and Ad- hoc requests

5.17.6.3. Proactively prevent and support resolution of data quality issues, improve query performance, and pro-vide report development coaching and guidance throughout the BI power user community

5.17.6.4. Communicate an understanding of the importance of compliance with corporate, regulatory, and internal security policies when administering and configuring the OBIEE/OBIA reporting platform

5.17.6.5. Help end-users and business analysts fully understand the technical options when solving business requirements and developing BI reporting solutions that enhance and extend the end-user usability experience

5.17.6.6. Prepare and present project reports for IT and Business management 5.17.6.7. Implement Policy and Standards

5.17.6.8. Perform Project Status

5.17.6.9. Perform Test plan preparation

5.17.6.10. Install and configure computer systems

5.17.6.11. Diagnose and solve hardware/software issues

5.17.6.12. Provide management/user in resolving complex automated support problems

Interfaces include but are not limited to: HTML; Hyperion; Visual Basic; JAVA; JavaScript VB Script; ASP; Perl; and CGI scripts, and applications will run under UNIX (Solaris), and Windows NT 4.0. HTTP connectivity will be hosted using Netscape and Microsoft IIS Web Servers. Applications will interface with Oracle 8 databases using Open Database Connectivity (ODC) and other application programming interfaces (API).

### 5.18. Computer Graphics

Provide graphics using applications such as Adobe Photoshop and Adobe Illustrator.

### 5.19. Technical Writers

The contractor shall provide qualified personnel to maintain and manage the yearly updating regulations, manuals, memorandums, and forms. The contractor shall submit all work products to the COR or designated Government representative for review and approval.

5.19.1 The contractor shall provide qualified personnel to type, review, edit, and publish e-documents, regulations, forms, and pamphlets utilizing Microsoft Excel, Share Point, PowerPoint, MSWord, Adobe Pro, Adobe Creative Suite, Lotus Forms, PDF Filler, and publication websites. Personnel will also review and edit business cards submitted by recruiting force. The contractor shall submit all work products to the COR or designated Government representative for review and approval.

5.19.2 The contractor shall establish filings and records IAW established DOD and USAREC guidelines.

5.19.3 The contractor shall receive and enter information into the web file database using Excel and Share Point.

### 5.21. Information Management Services

5.21.1. Provide office management, communication, and word processing support.

5.21.2. Provide support for the FOIA, Privacy Act, IT Records Management, IT Content Management, and IT HR Compliance Programs.

5.21.3. Receive and process inbound requests.

5.21.4. Verify documents that follow established regulations.

5.21.5. Work within designated systems of record to manage cases, documents, records, and other content. 5.21.6. Perform record searches.

5.21.7. Review and mark records as appropriate.

5.21.8. Generate responses to requests for Government approval and dissemination.

5.21.9. Maintain official office records, such as mail distribution lists and electronic signatures.

5.21.10. Maintain statistical and narrative data related to administrative services programs and generate reports.

5.21.11. Maintain awareness of policies, statutory law, regulations, organizational, and government-wide issues that impact the various Administrative Services Programs.

### 5.23. Administrative Support

The Contractor shall coordinate calendars to include setting and confirming appointments. Meeting preparation to include collecting and distributing read-a heads, appointment reminders, and connecting comms. Preparing documentation to include letters, memoranda, and briefings. Responsible for the completion and submission of the Daily Status Report (Perstat). Call screening. Task administration to include TMT Taskers, CIO tasks, Taskers, etc. Tracking mandatory training compliance for personnel, including updating DTMS and other systems of record. Attend administrative meetings, take minutes, and distribute minutes as necessary within three business days. Coordinate travel in DTS.

Hunatek provides administrative support, addressing the planning for execution of events. We coordinate meeting logistics, customer planning, and “dry run” sessions. Our support team creates required documentation for data calls, explanations, briefs and charts, PowerPoint presentations, and more, as needed. Hunatek corporate reach back means we have the SMEs for research, data retrieval/filtering/compilation and analysis as required. We will author analyses, presentations, notes, assessments, and other material on various technical topics, as required, for use by the USAREC. With technical writers and editors available, we can provide documentation support. We alway ensure deliverables in PDF format are Section 508 compliant, as well as any materials intended for publishing on the World Wide Web.

As a customer-centric organization, we have aligned our people and processes to support the evolving mission of our Government customers through a strategy that emphasizes: efficient use of corporate resources to add value to the customer and control costs, training and development of our personnel who deliver customer-focused solutions, ongoing communication with our customers to better understand their requirements, and use of technology-based tools to enhance our performance and reduce costs. Hunatek will provide PM support to attend USAREC team/staff meetings, customer planning, and dry run meetings. Hunatek manages and attends internal meetings and technical discussions, as required by our customers, to assist the government in organization of meetings, compiling notes, ensuring attendees are cleared appropriately, and facilitating other details of ensuring a well-run confab.

We provide logistic personnel to support the government operations, procurement and shipment of program material. We understand secure supply chain management and provide program support documentation. For numerous clients, our technologists assist in preparing and tracking requests for the purchase of hardware and software. Hunatek has provided research and technical documentation of equipment needed for support programs for various Navy operations, and we understand how to assist in the preparation of the material requirements of Navy operations.

Based on experience, Hunatek is able to provide superior inventory support for contract requirements and material tracking. We implement and manage asset management databases and monitor supply chain processes to track shipments for damage and duplication. We assist government in tracking vendor Return Material Authorization (RMA) numbers for return and repair items. Because of our expertise with asset management, we will maintain accurate inventory on all AV/VTC systems including spare parts. Track all maintenance activity and maintain sufficient spares on hand to affect rapid problem resolution for routine service issues. Our team will scan and electronically file documents as required, providing quality control for layout or technical drawings, security sign-off layout drawings, signed registration lists, letters of appreciation, awards, and facility and safe end-of-day check-out logs. On-site, we will coordinate with clients for reserving parking and installation access for their event attendees, presenters, and special guests (VIPs).

### 5.25. Cyber Security

Protect USAREC users, devices, systems, and data from unauthorized access or criminal use. through timely resolution of user requests, investigation of potential threats, user training programs, support for audits and inspections, and enterprise-wide communications/notifications/reporting. Serve as subject matter experts (SME) on common and advanced cyber topics as described below and liaison with external agencies, vendors, and key stakeholders to resolve cyber incidents, problems, and events.

5.25.1. Common USAREC Cyber support incidents may include Provisioning user accounts, ACTCS, REQUEST accounts, ACAS, Remedy, Social Media Threats, VIP reports, CAC registration, General Cyber Inquiries, User Violation Notifications, VIP Database Inputs.

Hunatek understands the needs of agencies for robust cyber security and information assurance (IA) (now transitioning to Cyber Security) programs. Hunatek has extensive experience in Cyber Security. Through work with the Department of Labor, the Defense Information Systems Agency (DISA), and the Federal Aviation Administration (FAA), we have had the opportunity to support this task area extensively for over a two decades. Supported areas include overall Information Assurance Program support. Elements include assistance with policy and planning development, selection of training and awareness information and accompanying learning management systems, operational integration of security into the software development life cycle (SDLC), operationalization of IA in an ITIL framework supporting Enterprise IT operations, automation of patching and mitigation through Windows Server Update Services (WSUS) servers (Windows environments) and YUM servers (Linux environments), control identification from the IA control knowledge base, protective system integration (host based security systems, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS)), enterprise antivirus client distribution, automated system log monitoring, network monitoring, operating system scanning (both Windows and Linux / Unix environments), certification and accreditation, Plan of Actions and Milestones (POA&M) development, Continuity of Operations Planning (COOP) where we have assisted customers in exercising all elements of their plans in simulations and simulations requiring practice of Disaster Recovery response activities. We provide scanning and vulnerability testing, penetration testing, exposure reduction through mitigation, evaluation of architectures for multi-vector exploit vulnerabilities such as can affect physical components of critical infrastructure, and certification and accreditation support activities. We understand the risk that a compromised infrastructure, enclave, network, system, or end user device can bring to an organization affecting anything from denial of services to employees and end user customers, to identify theft, or crippling of services or capabilities.

Our Approach: Our approach to providing Critical Infrastructure Protection and Information Assurance services is to ensure our personnel are well versed in the Federal requirements from the Federal Information Security Management Act (FISMA), and as available through National Institute of Standards and Technology (NIST) Special Publications, have appropriate certifications through accrediting organizations including ISC2, ISACA, and COMPTia, education, training, and experience to perform in roles where elevated privileges may be required to engage in provision of cyber protection activities. We then work to integrate security activities, including adoption of security services under the ITIL framework when appropriate with the operational and maintenance activities of the agency IT Enterprise. An effective security program involves active programs to have a Cyber Security Aware customer base, a trained and certified Cyber Security support staff, and cooperation in resources to identify and mitigate vulnerabilities in a timely manner.

Cyber Security: Deploy a multi-layer, defense-in-depth security architecture and a comprehensive security event management service via a security information management system. These tie into the overarching Enterprise Management Systems (EMS) providing a holistic view of the confidentiality, integrity, and availability of the monitored environment. Implement a common security infrastructure across all layers and domains to ensure only authorized and authenticated users gain access to critical information in compliance with FISMA. Our past performance has included cloud based security, messaging security, access control security, and persistence data at rest security.

### 5.26. Monthly Report

Summary of accomplishments during the reporting period and significant events. Deliverables submitted or progress on deliverable products. Any current or anticipated problems. Summary of activity planned for the next reporting period.

# Quality Control / Quality Assurance

1.6.1. Quality Control (QC): The contractor shall develop and maintain an effective quality control program to ensure services are performed by this PWS. The contractor shall develop and implement procedures toidentify, prevent, and ensure the non-recurrence of defective services. The contractor’s quality control program is how the contractor assures that work complies with the requirement of the contract. The contractor quality control plan shall be delivered to the contracting office no later than 15 days following contract award. After acceptance of the quality control plan, the contractor shall receive the contracting officer’s acceptance in writing of any proposed change to the QC system.

1.6.2. Quality Assurance: The government shall evaluate the contractor’s performance under this contract by the Quality Assurance Surveillance Plan. This plan is primarily focused on what the Government must do to ensure that the contractor has performed by the performance standards. It defines how the performance standards will be applied, the frequency of surveillance, and the minimum acceptable defect rate(s).

The HTGS-Culmen Team, comprised of HunaTek Government Solutions, Culmen International, and the Building People brings to A/OPR a comprehensive and unified commitment to quality. Each firm hold ISO 9001:2015 certifications, and Culmen International also brings Capability Maturity Model Integration (CMMI) Level 3 for Services, or CMMI-SVC Level 3.

**Process to Monitor Contract Performance and Schedule and Corrective Actions**

HTGS-Culmen's employs continuous communication with its employees, COR, and associated task order Government Task Managers (GTM) to monitor performance of its personnel on assigned to task orders. Our program and project managers are encouraged to pick up the phone: to be in regular voice communication with their direct contract reports and with their government counterparts. We’ve found the personal nature of a spoken conversation to be immensely helpful in building a trusted relationships that support open conversations needed to monitor performance. Often people are hesitant to voice minor items through written communication because tone is not easily communicated and/or the person is uncomfortable and/or doesn’t have time to put things in writing. This can lead to small items becoming issues because they are unknown. To address this our PM has regularly scheduled conversations as follows:

**Employees** – PM’s meet with their assigned contract personnel on a semi-weekly basis. Employees are encouraged to speak freely and that opinions shared will not be disclosed without employee’s permission unless there is an ethical obligation to do so. Topics covered during the conversation include: current focus and workload; accomplishments and accolades; issues and concerns; personal satisfaction; personnel asks for corporate support; upcoming personal time off; potential travel, etc. Relevant notes from the conversation are memorialized in the PM files. If the discussion included any counseling, the PM documents the counseling via written email to the employee and forwards a copy to human resources for inclusion in their file.

**Contracting Officer Representative (COR)** – Standing meetings are held with contract CORs on a semi-weekly basis. During these meetings the PM provides status personnel actions for incoming and outgoing employee on the contract, discusses open items and/or issues, and raises any new concerns. Additionally, the PM solicits feedback from the COR that they and/or GTM have expressed on assigned personnel. Relevant notes from the conversation are memorialized in the PM files with meeting notes/actions sent to the COR.

**Government Task Manager (GT**M) – Direct feedback from GTMs on personnel performance is often the most insightful as the employee’s performance directly impacts how the GTM meets their mission requirement. The PM will coordinate with the COR to establish regular meeting cadence with the GTMs to solicit temperature checks on personnel performance. We have found the more often these occurs the more proactive we can be heading off negative trends and rewarding and promoting high-performance.

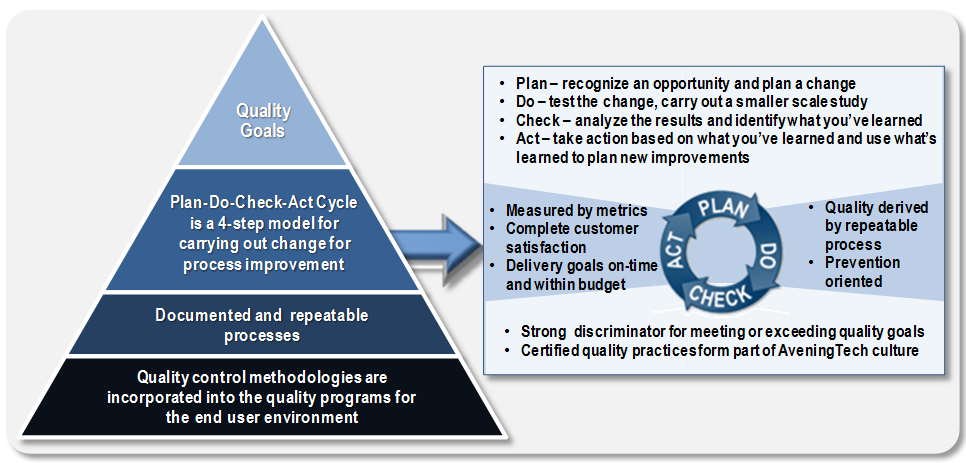
In addition to verbal communications COR and GTM, when allowed HTGS-Culmen utilizes surveys through automated providers. Surveys are designed to measure customer satisfaction of contractor’s performance on individual and management level and usually consist of 5-8 questions with multiple choice answers sent on a quarterly basis.

The goal of Hunatek’s Quality Management function is to verify that all deliverables meet all technical and performance requirements. Our QA procedures will be used to examine all deliverables and supporting materials to determine compliance with the Government’s requirements. The final version of the Quality Control Plan (QCP) will establish activities to be performed throughout the life cycle of this project. Hunatek management controls create the basis for our QC function, aiming to achieve defined goals within an established timetable. This has three components: (1) setting standards, (2) measuring actual performance, and (3) taking corrective action. A typical process for management control includes the following steps:

Actual performance is compared with planned performance

The difference between two is measured

Cases contributing to the difference are identified

Corrective action is taken to eliminate or minimize the difference.

Our QCP establishes basic approach to QA/QC processes and procedures. It is intended to verify that all services and deliverables submitted by Hunatek conform to the performance requirements and standards that have been established for the systems. DOTR Quality Assurance Surveillance Plan (QASP) in conjunction with Hunatek’s QCP and various other methods of assessing performance will be used by COTR and CO to perform on-site reviews and/or other types of verification to determine that the specified target performance requirements have been met.

Our QA efforts will be used to monitor and evaluate the adherence to the Government’s requirements and Hunatek’s Quality Management processes, procedures, and standards. This will determine potential work product and service quality. The QA function will establish the processes, procedures, and performance requirements for the systems. It will continuously monitor and audit the tasks product/deliverables against the established requirements, performance standards and processes. It will work to foster constructive communication, provide feedback to detect and prevent development problems, control risks, discuss alternative solutions, and ensure quality is built-in to all products. Overall, our QA activities will encompass: Product Audits, Process Audits, and QA Measurements and Analysis.

Quality Control (QC) practices involve measuring and monitoring specific project results to determine if they comply with project specifications and quality standards, and identify ways to eliminate causes of defects. QC practices should occur during product acquisition, product development, and throughout product change and operation. The QC activities will be identified and defined in the schedule and will be conducted by the QA team.

The key to successful delivery of quality work products and to the achievement of project performance standards are effective controls through reviews, testing and adherence to established processes. The first step in building a QCP with effective controls is defining the applicable standards the controls are required to meet. The establishment of standards sets the performance benchmarks for the project. On this contract, Hunatek will achieve the performance standards through the use of formal reviews. Our performance standards are based on achieving the contract objectives, analyzing issues, making recommendations and proposing solutions to complex organizational management issues that represent barriers to efficient and effective business. For each of the five Internet/Intranet Support tasks, our performance goal is to achieve a rating of “Excellent” in each of these performance goals:

Achievement of Contract Objectives

Achievement of Specific Task Requirements

Timeliness & Quality of Deliverables

Implementing effective controls involves defining appropriate reviews within the deliverable framework to integrate QCP procedures at the most beneficial time while allowing for any necessary corrective actions to occur without negative impacts to the project schedule. These reviews will be tracked and reported as milestones in the project BP. The reviews will ensure that the deliverables, schedule, resources and scope of the project are on track and that the deliverables meet the quality and performance standards established by the customer. These reviews ascertain the completeness, consistency, adequacy, accuracy and risks for the requirements, design and technical specifications of all off-line prototypes and system releases. Within this plan Hunatek will work closely with the Government on all work product releases to validate quality of content. Our quality control concept incorporates the daily execution of the project processes, periodic project status reviews with the client, and thorough review of the deliverables in concert with approved project standards.

Tying all of these processes together to create a quality delivery requires disciplined project controls. Each review tracked by our Project Lead will have defects recorded, reported, and corrected in a timely manner. A critical aspect of project controls is inter-group coordination and an approval work flow that ensures that impact analysis is performed to prevent a negative consequence on upstream or downstream data products.

Our risk management processes follow ISO 31000:2009 principles and DoD Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs (Jan 2017), which strengthens the likelihood of achieving requirements while improving identification of threats. We will use the qualitative risk assessment matrix (Table 29) for this effort.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Qualitative Risk Assessment Matrix  *Team Hunatek assesses, tracks and reports risk using a qualitative risk assessment matrix* | | | | | | |
| Likelihood | 5 - Near Certain (L > 90%) |  |  |  |  |  |
| 4 - Highly Likely (70% < L < 90%) |  |  |  |  |  |
| 3 - Likely (30% < L < 70%) |  |  |  |  |  |
| 2 - Low Likelihood (10% < L < 30%) |  |  |  |  |  |
| 1 - Not Likely (L < 10%) |  |  |  |  |  |
| Annotate Risk Number from Risk Register for each program risk, as mitigated in the appropriate cell. | | 1 | 2 | 3 | 4 | 5 |
| Minimal | Minor | Moderate | Major | Severe |
| Severity of Impact (“S”) | | | | |
| Severity of Impact (“**S**”) Definitions:  1. Minimal: A risk event that will have little or no impact on achieving outcome objectives.  2. Minor: As risk event that will have minor impact on achieving desired results, to the extent that one or more state outcome objectives will fall below goals but well above minimum acceptable levels.  3. Moderate: A risk event that will have moderate impact on achieving desired results, to the extent that one or more stated outcome objectives will fall well below goals but above minimum acceptable levels.  4. Major: A risk event that will have a significant impact on achieving desired results, to the extent that one or more stated outcome objectives will fall below acceptable levels. Performance unacceptable, significant changes required.  5. Severe: A risk event that will have a severe impact on achieving desired results, to the extent that one or more of its critical outcome objectives will not be achieved. Performance unacceptable, does not meet a key performance parameter. | | | | | | |

As part of our standard risk management process, we identify potential risks and mitigation actions upon receipt of the solicitation. This risk analysis continues throughout the contract’s PoP. Our analysis identifies distinct personnel risks associated with successful performance, assessing root causes, and then incorporating specific risk-elimination/mitigation plans within our approach.

| Minimizing Personnel Performance Risk  *Team Hunatek directly addresses the risks associated within each task enabling comprehensive support* | | | |
| --- | --- | --- | --- |
| Risk & Discussion | Initial  Risk | Hunatek Risk Mitigations | Residual  Risk |
| Transitioning | | | |
| During and after contract transition, personnel do not have the required skill sets or expertise to support testing, logistics, maintenance, and procurement activities. Supported units do not receive the required to support needed for mission accomplishment. Support is not effective and deliver support fails to meet the necessary conditions for planning to execute the required events. | S-3  L-4 | Hunatek validates that everyone is qualified and certified on the equipment, processes and procedures they support. As needed, we provide training to ensure personnel skills remain current and relevant. We implement comprehensive planning across each event, which mitigates performance risk. | S-2  L-1 |
| Recruiting and Retaining and Reach-Back | | | |
| Key/non-key personnel are not available due to sickness, health concerns or have scheduling conflicts with other test events. | S-3  L-4 | Hunatek uses our management approach to stretch existing personnel to fill short-term gaps. We recruit replacement personnel from within Hunatek to fill short term gap filling and we use our reach-back capability and tap into our bench of test professionals | S-2  L-1 |
| Managing Simultaneous Test Events | | | |
| Poor planning and resource management place simultaneous multi-test events at risk | S-3  L-4 | Hunatek uses our integrated and synchronized test planning/forecasting tool to anticipate personnel overlaps, hire surge personnel and use matrix management to share key personnel across test events. | S-2  L-1 |
| **S = Severity of Impact | L = Likelihood of Occurrence** | | | |

# Management Approach

1.6.9. Post Award Conference/Periodic Progress Meetings: The Contractor agrees to attend any post-award conference convened by the contracting activity or contract administration office by Federal Acquisition Regulation Subpart 42.5. The contracting officer, Contracting Officers Representative (COR), and other Government personnel, as appropriate, may meet periodically with the contractor to review the contractor's performance. At these meetings, the contracting officer will apprise the contractor of how the government views the contractor's performance and the contractor will apprise the Government of problems, if any, being experienced. Appropriate action shall be taken to resolve outstanding issues. These meetings shall be at no additional cost to the government.

HTGS-Culmen JV is comprised of two companies with extensive experience in managing complex and mission critical IT systems for our DOD clients that include, the U.S Army, U.S. Special Operations Command, and the U.S. Navy. Our overarching objective is to maintain a flat organizational structure that encourages decision making at the lowest possible level while still maintaining a level of control which ensures that compliance and quality are not compromised.

To facilitate management of this project, and ensure communication with USAREC stakeholders (a key to success, in our experience), Hunatek will draft a project plan that contains information on what software outputs (including documentation and other related material) are expected to be produced. We will define the functionality USAREC desired in detail, although this may change during the design review phase. We will identify who is responsible for releasing the software — our project manager or lead developer We will outline the process for revision control to be used, and detail how our revision control / configuration management system can be used by all members of the team will use]. Finally, the Hunatek project management plan will identify the software development model to be used; the external software that will be brought into the project, and the associated license requirements; what method will be used to accept each output (e.g. a specific user will review it); dependencies between outputs and with external dependencies; and major risks that might impact on the delivery of the work product.

Software development is one of the most challenging aspects of the IT Industry. Over the years Hunatek has mastered not only the art of organizing tasks but helping all members of the project team to realize their full potential and effectively collaborate toward the successful completion of a project.

Hunatek’s management and design team have solid experience in overseeing Internet and Intranet Web support activities. They continually monitor the staff’s activities, work with staff individually to facilitate learning and task success, and help to manage project risk through the careful pairing of resources to tasks.

Our team of experienced members has crafted a technical approach that is extremely scalable and effectively utilizes industry standard components to deliver on task orders. Our methodology includes reporting, oversight and quality control. Our task management life cycle comprises four phases: initiation, planning, execution and closure. Our step by step process includes the following:

* + During the initiation phase our team will designate a project manager who will coordinate with USAREC design team, oversee all requested changes, provide quality control and act as a liaison with USAREC.
  + During the planning phase we will cooperate with USAREC stakeholders to refine and define the goals and requirements.
  + During the execution phase we will build the deliverables and monitor and control all factors such as time, cost, risk, change and quality.
  + All project documentation will be managed by the team using an industry approved task management system (AtTask). Via this task management system, all team members will be able to enter and track project files, decisions, to-do lists, and more.
  + During final closure of task USAREC shall have ownership of all source files including images, audio, video, documentation and content used in the finished product.

Any successful project begins with a solid development plan. Hunatek’s design team utilizes a spiral-based development process, Rational Unified Process (RUP) to ensure the success of all our software development projects. This process provides a comprehensive roadmap that allows full control of the project through the various stages, flexibility to adjust as the needs of the project change and complete transparency.

Problem Reporting and Resolution: Effective problem reporting and corrective action procedures are critical to a successful project. The dynamics of the interaction between the various stakeholders will usually lead to an occasional problem or issue. Although this project encompasses elements of both maintenance and development for website content, this QCP will focus primarily on the procedures for handling problems encountered in development activities. The correction of maintenance problems will follow an expedited set of development procedures. The major difference is that maintenance problems usually occur in the production environment, require expedited handling and are not confined to the content development life cycle phase.

Problems are identified by various means and can be submitted by any stakeholder via telephone, e-mail, in a meeting, or formal testing results. Hunatek considers all of these problem submission methods legitimate and subject to the procedures defined in this QCP.

|  |  |  |  |
| --- | --- | --- | --- |
| **Task / Deliverable** | **Performance Standard** | **Performance**  **Threshold** | **Method of Surveillance** |
| Provide high quality research and deliverables | Each document created is well researched, documented, and prepared IAW professional technical writing standards. | All documents accepted by the government with no more than one revision. | Periodic Inspection  Select products will undergo 100% inspection. |
| Provide timely deliverables | All document, data, and reporting requirements are delivered IAW deliverable schedule or reporting schedule. | 95% on-time reporting and deliverables. Any delayed reports or deliverables were coordinated with the COR NLT two (2) weeks prior to scheduled delivery. | 100% inspection. |
| Provide Price/Cost control | Provide all PWS requirements IAW established Price/Cost limits. Minimize unnecessary TDY travel. | 100% compliance. | IPR Reviews. |
| Provide Quality Control | Contractor conducts quality control measures and documents plan progress IAW approved QCP. | 98% of all QC actions have been conducted and documented. | Periodic Inspection |

The types of inspection methods to be utilized by Hunatek to ensure Quality Control include the following:

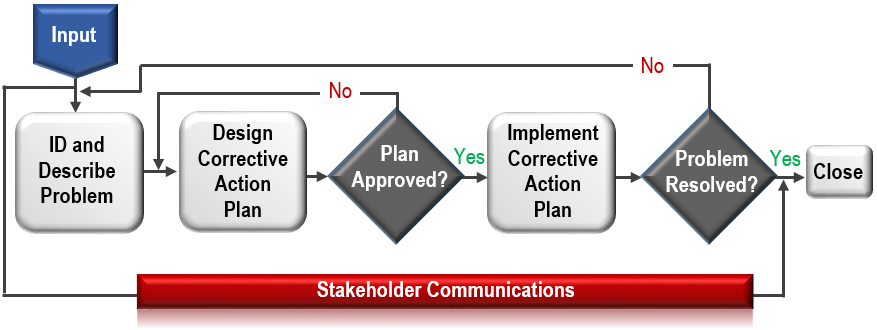
A. Planned (Structured) Inspections - Used to evaluate tasks or processes. These inspections are outlined in the PWS and applicable Government instructions.

B. Unscheduled (Unstructured) Inspections - Used to supplement planned inspections and effective in evaluating work of a routine or repetitive nature, e.g., checking content developed by Hunatek personnel for accuracy and completeness.

C. Random Sampling - Used to evaluate a portion of a task to estimate overall performance, e.g., software/license validation, database verification, and user system spot checks.

Hunatek also uses Validated Complaints to measure employee awareness of customer requirements. All customer complaints are investigated, reviewed, and responded to as quickly as possible. Responses include an explanation of the problem and the measures taken to correct the problem.

Hunatek understands that government surveillance of our performance is not limited to the Performance Objectives as outlined in the Performance Requirements Summary (PRS).

Four major steps, depicted in the following illustration, accomplish effective handling of a problem.

## Approach to Managing Personnel and Deliverables

HunaTek’s priority is to apply the right talent to the NOMB Program, leveraging, when possible, the valued incumbent staff currently providing programmatic support. At the Task Order level, we start with a breakdown and analysis of the technical requirements for the TO and develop a staffing plan for successful execution. This analysis includes an assessment of required knowledge, skills, and experience required for success, and results in a staffing plan that is effective, efficient, and aimed at delivering programmatic success. The labor and skill mix defined in the staffing plan then leads us to an assessment of current staff, when applicable, and any additional staffing needs required to bring the required expertise to the project. Our proven approach to hiring and retaining incumbent personnel consistently resulted in our successful of onboarding of Preferred Candidates for DOS and other customers. For our Office of the Judge Advocate General (OTJAG) IT Support Services (ITSS) program, our staffing plan resulted in the successful execution of 100% incumbent capture within five calendar days. These successes provide a high level of confidence that we will be able to hire and retain the desired staff. In addition to incumbent capture, HunaTek has an extensive recruiting program with the expertise to identify qualified, cleared staff with all required certifications for every position.

## Subcontractor Management

HunaTek, HTGS-Culmen JV’s managing member, is responsible for vetting each prospective subcontractor in accordance with its established ISO 9001:2015 contractor selection process. This process includes a determination of financial responsibility and an annual review of subcontractor performance. The HTGS-Culmen team brings all of the organic and organizational capabilities required to successfully execute the requirements for the USAREC ITSS program. While we intend to self-perform the vast majority of the contract, we remain open to bringing on additional partner expertise when we identify partners and capabilities that will deliver a strong value proposition to USAREC. Whether the value is derived from particular experience, expertise, or technical innovation, the HTGS-Culmen team’s subcontracting activities are designed to be transparent to USAREC.

HTGS-Culmen applies a “One Team” approach to ensure seamless performance regardless of company affiliation (Hunatek & Culmen. HTGS-Culmen has a successful track record of managing subcontractors and providing an integrated team. Our subcontractors will be required to adhere to all USAREC Guidelines and HTGS-Culmen policies and procedures, including meeting metrics of its QCP.

HTGS-Culmen emphasizes open, direct, and regular communications with subcontractors to monitor and manage performance. HTGS-Culmen will maintain privity of the contract (and restrictions) as the prime and the Government will not be involved in issue resolution associated with subcontractors or their personnel. Our focus will involve monitoring of all subcontracts to ensure compliance with the terms and conditions, completion of delineated milestones outlined in the Monthly Status Reports, and the timely submittal of required reports or deliverables. We will review invoices and expenses to ensure expenses are within budget, allowable, reasonable, and allocable. Furthermore, HTGS-Culmen’s PM will meet with each subcontractor individually, in addition to the team meeting, monthly. If issues arise, we will address them immediately.

As part of our “One Team” approach to subcontractor management, we seamlessly integrate all subcontractors into all project teams and activities. We continuously monitor and inspect subcontractor deliverables and hold our subcontractors accountable for performing all required activities to support HTGS-Culmen in meeting or exceeding all performance standards.

Each subcontractor performing under this effort will be required to provide a Monthly Status Report, similar in content and format to the HTGS-Culmen MSR, with their invoice, no later than 10 days after the end of each month.

HTGS-Culmen has established and maintains strong relationships within our executive leadership, conveying a shared commitment to the A/OPR Program. This level of corporate engagement and collaboration enhances visibility into program progress, allows for fair and timely dispute resolution, and allows each company to provide the required support to ensure program success.

Finally, we require our teammates to share their own quality best practices and lessons learned to customize our quality approach to the unique needs of USAREC. This allows HTGS-Culmen to bring our extensive collective experience and successes in delivering quality products and services, both at USAREC and throughout the federal government, to bear on successfully fulfilling each of the technical and schedule/delivery requirements identified in the SOW.

## Recruiting and Retaining Cleared, Qualified Personnel

We are adept in identifying and engaging experienced professionals with skills matching customer expectations. Our effective recruiting process includes finely honed steps for requirements such as certifications and clearances that enable us to hire quickly in response to critical staffing requirements. The effectiveness of our process is based on a dynamic and flexible approach to recruiting tailored to the unique needs of our clients, coupled with the experience of our recruiters.

**Table 4 -Recruiting Strategies & Approach**

|  |  |
| --- | --- |
| **Strategy** | **Approach** |
| **Incumbent Capture** | Leveraging the staff currently performing the work today, HTGS-Culmen has a proven process to recruit and retain priority personnel performing on the program today. Qualified existing personnel will be offered Right of First Refusal. |
| **Leverage major public resume databases and job boards** | We have access to resume subscriptions using the leading career search engines such as Career Builder, Monster, DICE, LinkedIn, and Clearancejobs.com. |
| **Use social networking sites** | We use social networking sites such as LinkedIn, Twitter, and Facebook both to source individuals and post open positions. |
| **Recruit locally** | We recruit locally using local area job fairs, user groups, local newspapers, and local universities. |
| **Maintain presence in local professional organizations** | We maintain a presence in local professional organizations such as PMI and other networking organizations |
| **Military Transition Assistance Programs** | We maintain relationships with local TAP offices and support our military personnel's transition to civilian. This supports expediting the on-boarding process since many of these candidates have the appropriate clearance and technical certifications required by the Government. |

Our recruiting strategies are driven to deliver to the mission and goals of the USAREC ITSS program, and so to is our posture toward talent retention. HTGS-Culmen’s ability to attract and retain highly qualified employees is a cornerstone of providing outstanding customer service. A key component of our successful retention strategy is a focus on increasing employee engagement. We consistently collect and analyze employee satisfaction using multiple means, including employee satisfaction surveys, benefits surveys, regular review meetings with program leads, town hall meetings with open dialogues, group- and one-on-one lunches with our corporate leadership. Opportunities for enhancements are elevated to the benefits committee.

Our Program and Project Management focus is oriented around the talent employed on our programs. Recognize the high cost of turnover to programs, both from a financial and performance standpoint, and we apply practices that are aimed at employee engagement and continued job satisfaction. To foster that workforce stability for USAREC, we work to maximize employee satisfaction through:

* Employee Recognition and Feedback - accomplished through our regular management/ employee meetings, team meetings, performance reviews, promotions, and on recognition via company email and/or our social media mechanisms.
* Monetary rewards (bonuses/ salary increases/spot awards).
* Regular market survey analysis of employee compensation to ensure competitiveness.
* Training and development programs.
* A work culture of respect and inclusion,
* Work-life balance. We provide employees with the ability to elect their schedules within the customer's margins to provide for their personal needs.
* Regular opportunities for employee feedback via surveys.

## Staffing Plan (1.2)

(5 page limit)

1.6.11. Key Personnel: The following personnel is considered key personnel by the Government: The contractor shall provide an on-site Program Manager who shall be responsible for the performance of the work. The name of this person and an alternate who shall act for the contractor when the manager is absent shall be designated in writing to the contracting officer. The Program Manager or alternate shall have full authority to act for the contractor on all contract matters relating to the daily operation of this contract. The Program Manager or alternate shall be available between 0730-1730, Monday thru Friday except on Federal holidays or when the Government facility is closed for administrative reasons.

1.6.12. Identification of Contractor Employees: All contract personnel attending meetings, answering Government telephones, and working in other situations where their contractor status is not obvious to third parties are required to identify themselves as such to avoid creating an impression in the minds of members of the public that they are Government officials. They must also ensure that all documents or reports produced by contractors are suitably marked as contractor products or that contractor participation is appropriately disclosed.

1.6.13. Contractor Travel: The contractor shall be required to travel to CONUS and OCONUS during the performance of this contract to attend events such as meetings, conferences, and training, and to provide technical support as required. OCONUS USAREC locations include Puerto Rico, Virgin Islands, Germany, Italy, Guam, American Samoa, Korea, and Japan. The contractor may be required to travel to off-site training locations and to ship training aids to these locations in support of this PWS. The contractor shall be authorized travel expenses consistent with the substantive provisions of the Joint Travel Regulation (JTR) and the limitation of funds specified in this contract. All travel requires Government approval/authorization and notification to the COR.

The purpose of the staffing plan is to make certain the project has sufficient staff with the right skills and experience to ensure a successful project completion. We stand ready to provide USDA with a full complement of personnel at contract start. We understand, however, that there are likely a number of incumbent personnel whose skills, qualifications and history of service add value to the program. Upon contract award, and before start-up, as members of the incumbent team, we will coordinate with the government to bring everyone up to speed on the plans for the program. This approach provides stability during contract start-up and is the most effective way to retain program knowledge and maintain continuity.

Hunatek understands that the contract tasks are extensive and require a streamlined and efficient approach that meets requirements while ensuring that best value is delivered to the government. This is a high profile/impact project that requires support on-site each working day. Our trained, certified and experienced PM will oversee this effort and the staff undertaking the various tasks. We are adept at providing cybersecurity consulting and quality assurance to ensure the vital functions of this effort continue to operate smoothly, whatever the circumstance. To provide comprehensive support, we have developed a lean team that addresses the entire range of requirements in the most efficient manner. The following exhibit defines the roles and responsibilities of our team over the broad categories of services.

## Security

1.6.7. Security Requirements: IAW AR 25-2 and HSPD-12, Installation Security Office will submit all background investigations on prospective contractors requiring CAC and/or network access. Provost Marshal’s Office wilconduct NCIC- III background checks on all other contractor personnel. For contractor personnel, the minimum requirement for access to unclassified federal information systems is as follows: IT-I access, a Single Scope Background Investigation (SSBI/SF 86); IT-II access, a NACLC (SF 86); and IT-III access, a NACI (SF 85P). Before CAC issuance, the NAC (FBI 10-point FBI fingerprint check) must be completed without adverse comment, and the NACI or equivalent must be initiated. CACs will not be issued before the fingerprint check results have been completed and the investigation has been submitted. Fingerprints and the appropriate investigation will be submitted by the Government.

1.6.7.1 Status of Forces Agreement (SOFA). Contractor shall comply with the provisions of current SOFAs of host nations identified in the PWS.

1.6.7.2. PHYSICAL Security: The contractor shall be responsible for safeguarding all government equipment, information, and property provided for contractor use. At the close of each work period, government facilities, equipment, and materials shall be secured.

1.6.7.3. In the event keys, other than master keys, are lost or duplicated, the Contractor shall, upon the direction of the Contracting Officer, re-key or replace the affected lock or locks; however, the Government, at its option, may replace the affected lock or locks or perform re-keying. When the replacement of locks or re-keying is performed by the Government, the total cost of re-keying or the replacement of the lock or locks shall be deducted from the monthly payment due to the Contractor. In the event a master key is lost or duplicated, all locks and keys for that system shall be replaced by the Government, and the total cost deducted from the monthly payment due to the Contractor.

1.6.7.4. The Contractor shall prohibit the use of Government-issued keys/key cards by any persons other than the Contractor’s employees. The Contractor shall prohibit the opening of locked areas by Contractor employees to permit the entrance of persons other than Contractor employees engaged in the performance of assigned work in those areas, or personnel authorized entrance by the Contracting Officer.

1.6.7.5. Anti-Terrorism and Information Assurance Training.

1.6.7.6. AT Level I Training: All contractor employees, including subcontractor employees, requiring access to Army installations, facilities, and controlled access areas shall complete AT Level I awareness training within 30 calendar days after the contract start date or the effective date of incorporation of this requirement into the contract, whichever is applicable. The contractor shall submit certificates of completion for each affected contractor employee and subcontractor employee, to the COR or the contracting officer, if a COR is not assigned, within 30 calendar days after completion of training by all employees and subcontractor personnel. AT Level I awareness training is available at the following website: https://jkodirect.jten.mil/.

1.6.7.7. AT Awareness Training for Contractor Personnel Traveling Overseas: US-based contractor employees and associated sub-contractor employees to make available and receive government-provided area of responsibility (AOR) specific AT awareness training as directed by AR 525-13. Specific AOR training content is directed by the combatant commander with the unit ATO being the local point of contact.

1.6.7.8. Access and General Protection/Security Policy and Procedures: Contractor and all associated sub-contractor’s employees shall comply with applicable installation, facility, and area commander installation/facility access, and local security policies and procedures. The contractor shall also provide all information required for background checks to meet installation access requirements to be accomplished by the installation Provost Marshal Office, Director of Emergency Services, or Security Office. The contractor workforce must comply with all personal identity verification requirements as directed by DOD, HQDA, and/or local policy. In addition to the changes otherwise authorized by the changes clause of this contract, should the Force Protection Condition (FPCON) at any individual facility or installation change, the Government may require changes in contractor security matters or processes.

1.6.7.9. iWATCH Training: The contractor and all associated sub-contractors shall brief all employees on the local iWATCH program (training standards provided by the requiring activity ATO). This locally developed training will be used to inform employees of the types of behavior to watch for and instruct employees to report suspicious activity to the COR. This training shall be completed within 60 calendar days of contract award and within 30 calendar days of new employees commencing performance with the results reported to the COR NLT 30 calendar days after contract award.

1.6.7.10. Contractor Employees Who Require Access to Government Information Systems: All contractor employees with access to a government info system must be registered in the ATCTS (Army Training Certification Tracking System) https://atc.us.army.mil/iastar/index.php at the commencement of services and must complete the DOD Information Assurance Awareness before access to the information systems and then annually thereafter.

1.6.7.11. Global Address Listing (GAL): All contract employees who require access to Government Information Systems shall update their profile and Global Address Listing (GAL) information: https://www.dmdc.osd.mil/milconnect within 10 working days of being granted IT access.

1.6.7.12. OPSEC Training: Per AR 530-1, Operations Security, the contractor employees must complete Level I OPSEC Awareness training. New employees must be trained within 30 calendar days of their reporting for duty and annually thereafter.

1.6.7.14. Threat Awareness and Reporting Program (TARP). DA contract employees possessing a security clearance shall receive annual TARP training instructed by a CI agent or other trainer as specified in AR381-12,2-4b. Training shall be accomplished annually during the organization's scheduled TARP training session. In those instances where live training is not possible, such as in deployed theaters of operation, CI units may, in coordination with appropriate commanders, develop alternative means to conduct threat awareness training and meet the requirements of this AR 381-12.

1.6.7.15. Information assurance (IA)/information technology (IT) training: All contractor employees and associated sub-contractor employees must complete the DoD IA awareness training before issuance of network access and annually thereafter. All contractor employees working in IA/IT functions must comply with DoD and Army training requirements in DoDD 8570.01, DoD 8570.01-M, and AR 25-2 within 30 days of starting employment.

1.6.7.16. Annual Cyber Awareness Training: All contractor employees, including subcontractor employees, requiring access to Army installations, facilities, and controlled access areas shall complete the Annual Cyber Awareness Training located at the US Army IA Training Center website listed below (previous training expires 25/Nov/13): Link: https://ia.signal.army.mil/DoDIAA/default.asp.

1.6.7.17. Acceptable Use Policy: All contractor employees, including subcontractor employees, requiring access to Army installations, facilities, and controlled access areas shall complete a new Acceptable Use Policy (Annual Requirement) at the same website: Link: https://ia.signal.army.mil/DoDIAA/default.asp. (Click “Login”, Log in with CAC, confirm the information on-page, and click on “View and Sign AUP”.

1.6.8. Special Qualifications: All contractor employees shall adhere to the requirements of DoDD 8570.01- M and AR 25-2 training and qualification requirements for each position classification. Contractors shall obtain any certifications inherent with job/position functions. We will ensure that individuals check their training profile on the ATCTS site.

5.27.1. By DOD Regulation 8570.01-M paragraphs C1.4.4.12, C7.3.4.4, C1.4.4.5, C2.1.5, C1.4.4.12, C3.2.4.8.1 and C4.2.3.1, contractor employees with privileged access to any information system, contractors performing described Information Assurance (IA) functions must satisfy both preparatory and sustaining DOD IA training and certification requirements. Any personnel hired to perform functions in a position deemed as requiring elevated access privileges must be able to attain the security background check needed for the functions required. There are other determining factors regarding whether a user is placed in one of these training groups. Ensure staff have Approved Baseline Certifications. 5.27.2. The following certifications have been approved as IA baseline certifications for the IA Workforce for IAT Level II. Personnel performing IA functions must obtain one of the certifications required for their position category or specialty and level. IAT Level II: CCNA Security; CySA+ \*\*; GICSP; GSEC Security+ CE; CND; SSCP

HunaTek holds a Top-Secret level facility clearance as required for contract performance in accordance with the DD Form 254, Department of Defense Contract Security Classification Specification. To meet the security requirements for this program, we will ensure all personnel have been vetted with the required background check and hold the appropriate level of Security Level Clearances.

Since it will be necessary for some HTGS-Culmen personnel to have access to classified material and/or to enter into areas requiring a security clearance, each contractor employee requiring such access will have an individual security clearance commensurate with the required level of access prior to contract performance. HTGS-Culmen's Human Resource departments follows a standard process for vetting every candidate who applies for a job. We start by reviewing resumes against the position requirements, perform initial phone screenings, and then conduct candidate interviews. Our process, as detailed in Figure 4 - Candidate Recruiting & Vetting Process, also includes criminal background checks. For positions that require cleared personnel, our FSO conducts an initial clearance verification as part of the vetting process. If a candidate is being sponsored for a clearance, this will occur after the candidate signs their contingent offer letter. HTGS-Culmen takes ownership of all personnel’s clearances within Defense Counterintelligence and Security Agency (DCSA) Defense Information Security System (DISS) as part of its onboarding process. Our personnel our committed to compliance with all required training related to current Information Assurance, Operational Security (OPSEC) Awareness, and Antiterrorism (AT) postures.

Hunatek takes a holistic approach to cybersecurity program management. As part of our open line of communication, Hunatek will provide regular (weekly, monthly) status reports and coordinate meetings with government stakeholders. We will build Executive Dashboards and support creation of maintenance of web sites as needed. We will define and develop IT Security standards, metrics/key performance indicators (KPI), policies, process, procedures, templates and artifacts. Our approach is to partner with the agency to maintain open lines of communication and ensure effective program management. We recommend a Program Management Office model: a cybersecurity PMO will address major components: Risk Management, Compliance, Policy and Procedure Management, Vulnerability Management, Security Project Management, Security Metrics and Knowledge Management. Hunatek has found that routine monitoring is necessary to quickly detect malicious, undesirable, or abnormal activity. It is less costly to be proactive than to wait until end users, law enforcement, or the press provides notification of a breach.

Our approach to cybersecurity compliance support sets Hunatek apart. Our risk management is based on NIST’s Risk Management Framework principles: identification, evaluation, and mitigation. We identify risks, analyze impact of each identified risk, and then take counter measures for the identified and analyzed risks. Hunatek implements a Risk Management Plan (RMP) that provides solutions for mitigating anticipated problems (or risks), a proactive methodology for detecting and resolving unforeseen risks, and a means to track and communicate them to the government in a timely manner.

We support the fundamental purpose of the certification process, to determine if the security controls for an IT system are correctly implemented and are effective in their application. We are thus able to apply NIST 800- 53A “Assessing Security and Privacy Controls in Federal Information Systems and Organizations” with our proven processes for conducting security assessments on controls after system updates or changes.

After conducting a comprehensive risk assessment, our team is able to develop system security plans that explain who, what, how, and how often for each security control (leveraging common or inherited controls where possible). Our teams also develop all supporting documentation, such as eAuthentication Risk Assessments, Privacy Impact Assessments, IT Contingency Plans, Security Control Assessment/Test Plans, Security Assessment Reports, ATO Letters, and agency-specific documentation. Hunatek will compose and deliver Risk Assessment Reports (RAR), Security Assessment Reports, and POA&M documents in support of new information system being developed in order to achieve system ATO within 30 days.

Hunatek cyber specialists develop the SSP in accordance with the guidelines contained in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18, Guide for Developing Security Plans for Information Technology Systems, and applicable risk mitigation guidance and standards. We will perform Plans of Action and Milestones (POA&M) and risk management oversight on all USDA RD contractor and cloud-based systems — an RMF POA&M is a living document designed as a management tool. Hunatek understands that it is important to track these vulnerabilities in a comprehensive way using POA&Ms. Using the Hunatek methodology, the POA&M task is ongoing from accreditation to decommission of all systems, documenting each vulnerability found on a system that cannot be remediated within 30 days.

The team’s approach to cybersecurity policy rests on defining compliant policies and ensuring compliance. Compliance with internal standards and policies or regulatory requirements, can be a major issue for any information security program. It is also a risk that must be managed and can consume a large percentage of information security resources. Hunatek successfully implemented Vulnerability Assessment and Data Protection policies and other PII memo and road maps at USDA NRCS. Hunatek will understand the USDA RD need and compliance regulations and will make an inventory of all the current policies. Once we understand all the current policies, our team will recommend any new policies that might be missing and will help with the creation of the new policies. Hunatek understands the need for a Vulnerability Assessment policy and a Data Protection Policy which goes in hand with the PII memo and Clean desk policy.

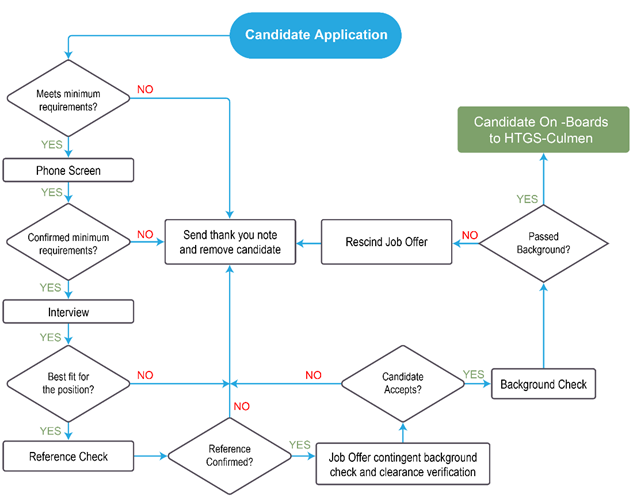


Figure 4 - Candidate Recruiting & Vetting Process

Classified material received or generated in the performance of this contract shall be safeguarded and disposed of in accordance with the National Industrial Security Program Operating Manual (DOD 5220.22-M).

## GFI/GFP

1.6.15. Data Rights: The Government has unlimited rights to all documents/material produced under this contract. All documents and materials, including the source codes of any software, produced under this contract shall be Government-owned and are the property of the Government with all rights and privileges of ownership/copyright belonging exclusively to the Government. These documents and materials may not be used or sold by the contractor without written permission from the Contracting Officer. All materials supplied to the Government shall be the sole property of the Government and may not be used for any other purpose. This right does not abrogate any other Government rights.

3. GOVERNMENT-FURNISHED ITEMS AND SERVICES:

3.1. Services: None.

3.2. Facilities: The Government will provide the necessary workspace for the contractor staff to provide the support outlined in the PWS to include desk space, telephones, computers, and other items necessary to maintain an office environment.

3.3. Utilities: The Government will provide all utilities required to perform under this contract. The contractor (to include sub-contractors) shall instruct employees in utility conservation practices. The contractor shall be responsible for operating under conditions that preclude the waste of utilities, which include turning off the water faucets or valves after using the required amount to accomplish cleaning vehicles and equipment.

3.4. Equipment: The Government will provide the necessary computing and telecommunications equipment to perform services under this PWS.

3.5. Materials: None

4. CONTRACTOR FURNISHED ITEMS AND RESPONSIBILITIES:

4.1 General: The Contractor shall furnish all necessary supplies, equipment, and services required to perform work under this contract that is not listed under Section 3 of this PWS.

HTGS-Culmen JV’s committed to managing, preserving, protecting, and maintaining all Government Furnished Information (GFI) and Government Furnished Property (GFP) in compliance with the very strict standards expected by the Government. Employees receive Property Management training in line with his/her assigned responsibilities. Each employee in turn assumes responsibility for all property assigned to them or under their individual area of responsibility, whether via hand receipt or assumed with position responsibilities. HTGS-Culmen JV preserves Government property by verifying that all personnel are trained and licensed/certified for the vehicle or equipment they are assigned to IAW DOD 4500.36-R. Our employees (and subcontractors) acknowledge agree to follow all applicable policies, procedures, SOPs, Work Instructions (WI), or guidance from our PM or ISD Manager.

HTGS-Culmen JV understands the importance of sensitive and controlled items and the heightened trust the USG has in any contractor tasked with managing, controlling, and maintaining 100% accountability of sensitive and controlled items. HTGS-Culmen JV will employ controls for all employees who handle, control, or are responsible for sensitive or controlled items. These employees possess higher security clearances and receive additional training to effectively control and maintain 100% accountability for sensitive and controlled items.

The Hunatek Program Manager will oversee the management of Government Furnished Equipment/Government Furnished Property (GFE/GFP), including secure inventory control of all assets, and adherence to requisite DOD data protection regulations and rules. We have established SOPs for asset management and inventory control process flow, detailing the steps we take to ensure secure supply chain management of supplies, materials, parts and equipment to meet contractual requirements. Concerning Government Furnished Property (GFP), Hunatek will apply our standardized processes for receiving, tracking, inventorying, and handling of GFP.

## OCI

1.6.16. Organizational Conflict of Interest: Contractor and subcontractor personnel performing work under this contract may receive, have access to or participate in the development of proprietary or source selection information (e.g., cost or pricing information, budget information or analyses, specifications, or work statements, etc.) or perform evaluation services which may create a current or subsequent Organizational Conflict of Interests (OCI) as defined in FAR Subpart 9.5. The Contractor shall notify the Contracting Officer immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI and shall promptly submit a plan to the Contracting Officer to avoid or mitigate any such OCI. The Contractor’s mitigation plan will be determined to be accepted solely at the discretion of the Contracting Officer and in the event, the Contracting Officer unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the Contracting Officer may affect other remedies as he or she deems necessary, including prohibiting the Contractor from participation in subsequently contracted requirements which may be affected by the OCI.

Per the PWS, Hunatek states inequitably that Organizational and Consultant Conflicts of Interest (OCCI) as described in FAR 9.5 do not exist for our organization. We are certain no OCCI exists, and the following details to support our position. Hunatek nor and any of its subcontractors have financial business or contractual relationship with contractors and/or subcontractors that are engaged in maintenance or development of the subject systems. Hunatek maintains a corporate Conflict of Interest policy that requires all staff to report (a) a conflict (or who think they may have a conflict) and to disclose the conflict/potential conflict, and (b) prohibit interested staff from participating in any matter in which there is a conflict. If this situation changes, Hunatek will immediately notify the Contracting Officer and we will submit an OCCI plan within seven days of discovery of such a situation, explaining in detail how the OCCI will be mitigated and/or avoided.

HTGS-Culmen, through their respective program portfolio, does not currently have any instances of real or perceived Organizational Conflicts of Interest (OCI). Throughout the course of program performance, we remain vigilant around OCI avoidance to the maximum extent possible, and upon any concerns around OCI arising we will immediately notify the Contracting Officer and commence planning for an appropriate mitigation approach.

# Transition

1.6.17. PHASE IN /PHASE OUT PERIOD: To minimize any decreases in productivity and to prevent possible negative impacts on additional services, the Contractor shall have personnel on board, during the 30-day phase-in / phase-out periods. During the phase-in period, the Contractor shall become familiar with performance requirements to commence full performance of services on the contract start date.

Hunatek initiates our project staffing activities as early as practical within the contract process to fill key positions, as well as meet and exceed customer requirements. Consequently, transition planning and execution is a critical aspect to our process and will start even before the required on-site transition plan meeting. Our goal on day one is to meet all our customer’s requirements, while continually expanding our capabilities as quickly as possible. To accomplish this, we work collaboratively with our customers, and any existing incumbent. An essential priority is gaining a full understanding of our customer’s current and desired operational needs, mission requirements, and organizational vision. In addition, our transition team captures and analyzes ongoing projects and initiatives, processes, systems and tools in use, as well as organizational culture. Our team also coordinates with any existing incumbents for a transfer of knowledge that includes but is not limited to the status of IT systems and architecture supported, ongoing initiatives and projects, as well as additional staffing insights. Our planning purpose is a smooth handoff of responsibilities to ensure no impact to our customers.

Once our team gathers all our required data, and completes its initial analysis, we will establish a comprehensive plan leading up to contract transition and covering the first 30 days of execution. A key element of the plan is retaining incumbent personnel that are well regarded and excellent performers. In addition, this plan will identify any potential capability gaps so we can enact plans to mitigate them. This mitigation will include addressing any staffing shortfalls. In the event our team is unable to retain an existing incumbent or recruit a new team member in accordance with our transition timeline, Hunatek will temporarily reallocate one of our personnel to the required customer site until a suitable permanent team member is brought on board.

Part of our Phase-In Plan is based on our extensive past performance — by selecting Hunatek, the Government will continue to work with a high value partner who is intimately familiar with the vision of the organization, its mission, the day-to-day working environment; and current and emerging trends in customer data acquisition needs. Hunatek will continue to leverage our experience overseeing this project and providing the technical support, planning and quality control, knowledge management innovation the Government has come to expect from us.

By keeping the steady state and retaining Hunatek, the Government can ensure knowledge transition is minimal. This is critical for all stages of the data gathering and analysis life cycle. Because of this, Hunatek does not require a transition period — we are already in place. But Hunatek’s team will take advantage of the transition period to make improvements. Hunatek will leverage the transition period as an opportunity to raise the bar of expectations — we will craft a plan for new procedures and improvements, and deliver within ten days of contract award. After the Government approves, we will implement new procedures.

Transition Risk Management and Mitigation. Hunatek understands that Risk Management Plan is one of the key factors to a successful transition. We will use a formal risk management methodology that identifies risk, access probability of occurrence, and develop a risk mitigation plan. The following exhibit lists transition-related risks and their mitigation strategy that Hunatek anticipates as part of the transition.

|  |  |
| --- | --- |
| **Transition Risk** | **Mitigation Strategy** |
| Transition to a new contractor may result in the loss of key personnel skills/knowledge; uncooperative incumbent. | Work with the government to identify and on-board key incumbent personnel; debriefing key personnel to obtain important information. |
| Ability to rapidly assemble a highly  skilled staff in a timely manner to satisfy requirements. | Proactive approach to capturing qualified incumbent staff; already have qualified staff in place to start work at the performance start date; maintain a large queue of pre-qualified personnel to back-fill vacancy. |
| Ability to manage on-site staff (contractors/sub-contractors). | Single point of management where Hunatek operates as a seamless team. |