



U.S. AIR FORCE
PERFORMANCE WORK STATEMENT (PWS)

For

MAINTENANCE AND DEVELOPMENT

Of

Hazardous Communication/Electronic Site Safety Workbook

AIR FORCE MATERIAL COMMAND (AFMC)
OGDEN AIR LOGISTICS COMPLEX (OO-ALC)
75TH AIR BASE WING (75 ABW)

TABLE OF CONTENTS

1.0 DESCRIPTION OF SERVICES.....	1
1.1 OVERVIEW	1
1.2 SCOPE	2
1.3 REQUIRMENTS	2
1.3.1 Software Development	2
1.3.2 Requirements Management	2
1.3.3 Database Management	3
1.3.4 Web Development	4
1.3.5 Content Management	4
1.3.6 Software Engineering	4
1.3.7 Application Functionality Testing and Vulnerability Mitigation.....	5
1.3.7.1 Application Information Security.....	5
1.3.8 Systems Architecture.....	6
1.3.9 Configuration Management.....	6
1.3.10 Resource Management	7
1.3.11 Program Management	7
1.3.11.1 Program Records	7
1.3.11.2 Technical Support.....	7
1.3.11.3 Additional Responsibilities	8
1.4 Document Requirements	8
1.4.1 User’s Guide.....	8
1.4.2 Test Evaluation Master Plan (TEMP)/Test Cases.....	8
1.4.3 Source Code	8
1.4.4 System Release Packages	9
2.0 SERVICE DELIVERY SUMMARY (SDS)	9
3.0 GOVERNMENT FURNISHED PROPERTY	10
3.1 General	10
4.0 GENERAL INFORMATION.....	10
4.1 Transition Period/Orientation.....	10
4.2 Phase In/Out	11
4.3 Travel Requirements	11
4.4 Security Requirements	11
4.4.1 Information Assurance (IA) Technical Considerations.....	11
4.4.2 Access to Hill AFB.....	11
4.5 Access to the Base Network.....	12
4.6 Physical Security	13
4.7 Non-Disclosure.....	13
4.8 Quality and Safety	14
4.9 Quality Control.....	14
4.10 Quality Assurance	15
4.11 Contracting Officer’s Representative (COR).....	15

4.12 Hours of Operation	16
4.13 Conservation of Utilities	16
4.14 Government Observations	16
4.15 Safety Requirements	17
4.16 Publications	17
4.17 Freedom of Information Act (FOIA)/Privacy Act	17
4.18 Operational Security (OPSEC).....	17
APPENDICES	18
Appendix A - Hazcom/eSSWB Required Level of Expertise.....	18
Appendix B – Mandatory Guidance and Policy.....	20
Appendix C – Safety Management Plan	21
Appendix D - CDRLs.....	25
Appendix E - Acronyms.....	26

1.0 DESCRIPTION OF SERVICES

1.1 OVERVIEW

HazCom: HazCom is an automated web-enabled system that provides users with the most up-to-date regulations and guidance to comply with the Environmental Protection Agency (EPA), Occupational Safety & Health Administration (OSHA), Federal, State, local, and union standards. HazCom allows users to personalize and tailor required information to meet specific needs, such as: worker access to work area hazards, emergency response, personal protection information, safety, environmental requirements, spill requirements, and all future requirements that OSHA, EPA, Federal, State, local, and union deem necessary and mandatory. The contractor shall comply with Rehabilitation Act of 1973 Section 508, OSHA, AF, AFMC and HAFB requirements. The contractor shall update shop Potential Exposure Group (PEG) listings and maintain the list of employees impacted by those PEGs. The contractor shall provide train-the-trainer level training to users as needed. The contractor shall update, validate and maintain user manual, developer manual and leadership manual to reflect the current state of the application.

Hill Air Force Base (AFB) houses over 10,000 products at over 65 major locations that contain over 7,000 chemicals and 14,000 people, in over 130 buildings that impact over 230 Potential Exposure Groups (PEGs) impacting more than 5,000 users. Paper products that support these organizations have not upgraded to the HazCom System, are constantly out of date, and are increasingly more expensive to build and maintain. The contractor will continue to deploy and maintain the HazCom portal to automate, web-enable, personalize and tailor required information to meet the users' needs.

Electronic Site Safety Workbook (eSSWB): eSSWB is an automated web-enabled system that provides users with the most up-to-date job safety training as provided in general by the safety office and specifically by the supervisor. eSSWB is used at OO-ALC as well as various Geographically Separated Units (GSUs) and allows users to personalize and tailor required information to meet specific needs, such as: worker access to work area hazards, specific safety program information and guidance, safety related training, emergency response, personal protection information, environmental requirements, and all future requirements that OSHA, Air Force, Federal, State, local, and union deem necessary and mandatory. The contractor shall comply with Rehabilitation Act of 1973 Section 508, OSHA, AF, AFMC and HAFB requirements.

The Ogden Air Logistics Complex (OO-ALC) employs over 700 supervisors who oversee over 8,000 people, in over 130 buildings that impact over 300 worksites. The eSSWB application provides the administration and production managers, supervisors, and employees with safety information related to their specific worksite and gives them the ability to access other worksite hazards as well. The robust system also allows Commanders to see the status of their safety program by showing them a breakdown of each sites compliance with their program.

The goal of this effort is to support the mission of the Department of Defense, the Air Force, Air Force Materiel Command (AFMC), and HAFB by applying information technology components to meet present and future knowledge-management requirements. This goal is driven by the increasing reliance on computer information systems to provide linkage between all elements of the work force, work processes,

information content, and decision-making, as well as, the requirement to manage, store, retrieve, manipulate, and process key data necessary to the efficient and effective execution of operations. The contractor shall ensure that all analysis design, development and maintenance tasks shall be completed on time in accordance with normal business hours.

1.2 SCOPE

The contractor shall work with OO-ALC/SE, through 75ABW/SC, to support the functional capabilities of the specific services in the listed tasks including software sustainment, maintenance, (possible enhancement of existing applications HazCom/eSSWB) and development of safety and occupational health information delivery systems such as activities associated with HazCom/eSSWB. This shall include updates as required to any technical documents and any new documentation.

1.3 REQUIRMENTS

1.3.1 Software Development

The contractor shall:

- perform and document explicit and implicit functional and technical requirements, create analysis and design documentation, create program specifications, and unit test criteria, code and test program units, and produce program documentation.
- use applicable structured software development and object-oriented principles and tool suites and adhere to established software development standards and guidelines as prescribed by Capability Maturity Model (CMM), Capability Maturity Model Integration (CMMI), Institute of Electrical and Electronics Engineers (IEEE), and International Organization for Standardization (ISO).
- develop, test and integrate software utilizing CMMI practices, processes and services.
- follow applicable 75 ABW/SC Configuration and Change Management policies developed in accordance with CMMI, IEEE and ISO; including source code management utilizing the 75 ABW/SC standard software repositories. This includes working with limited direction on complex assignments; the contractor is typically responsible for independently defining approach to tasks and solutions to problems.
- perform in accordance with DOD, Air Force, and AFMC architectures, policies and standards, including the Global Combat Support Systems (GCSS) architecture.
- perform in accordance with integrating Hypertext Markup Language (HTML and/or HTML5), Cascading Style Sheets (CSS and/or CSS3), Extensible Markup Language (XML), Ajax, C #, Visual Basic code, Entity, Model View Controller (MVC), JSON, SQL Server Reporting Services, IIS, Bootstrap, Backbone, Web Service, REST Services, SSIS, Angular JS, and Structured Query Language (SQL and/or T-SQL) within the Microsoft.NET environment.

1.3.2 Requirements Management

The contractor shall:

- perform requirements management to include gathering requirements and maintaining requirements traceability.
- if funded entirely or in part by AFMC headquarters the contractor shall use Information System Management Tool (ISMT), an AFMC requirements management tool. This will be the single tracking point for requirements documentation, approval to work, testing,

and deployment (CDRL A002). If not funded by AFMC headquarters, the requirements management tool used by 75 ABW/SC will be the alternate authorized system.

- perform configuration management by gathering and tracking requirements, and conducting analysis, design, and engineering of new requirements.
- translate project requirements to design modifications maintaining the integrity of the product's design.
- develop user scenarios, user interfaces, and provide oversight of development activities.
- provide the technical expertise required to understand the business processes of HazCom/eSSWB to enhance the functional capabilities of support for the operations, maintenance, and sustainment of the system.
- provide business process-improvement support that includes all activities involved in helping improve customer data systems through business processes including rethinking program design and aligning information technology infrastructures with business missions, goals, and objectives.
- use Microsoft SharePoint in recording and distributing business process-improvement processes and information.
- provide organizational facilitation support including aiding and building cross-functional teams within organizations and components of organizations.
- perform manual and automated modeling activities, including requirements, processes, activities, and data.
- perform business process reengineering.
- create data flow diagrams, perform data standardization, and perform enterprise modeling, functional economic analysis, simulation/modeling, activity based costing and activity based management support.
- provide "to-be" functional analysis using statistical methods, comparative analysis, timeline analysis, cross-functional analysis, and cause and effect diagrams.
- evaluate suitability of business process improvement tools and methodologies.
- acquire, install, and utilize such tools and methodologies in conducting business process improvement tasks.

1.3.3 Database Management

The contractor shall:

- use the most current and available version of "Microsoft SQL Server" Enterprise Manager, and shall be proficient in Windows Server platforms, be proficient in SQL and Transact SQL development, debugging, and performance tuning activities.
- use the most current version of "Microsoft SQL Server" database. The contractor shall properly document all designing, modification and additions made to any code through most current Air Force approved tracking system.
- ensure that all SQL code is optimized for performance and written according to standard described in CDRL A003. No more than 10% unplanned downtime monthly within the database application.
- possess the knowledge and ability to design, implement and manage an enterprise level database.
- design data distributions and data archiving solutions with security measures in place to protect against computer threats.

- possess the ability to produce entity relationship and data flow diagrams, database normalization schemas that are logical to physical data maps and data table parameters.
- be responsible for data integrity and availability for enterprise level databases, tables and structures.

1.3.4 Web Development

The contractor shall:

- perform planning, design, development, test and implementation of various static and dynamic content web sites for web services technologies.
- maintain expertise, as defined in Appendix A, in computer information systems to provide linkage between all elements of the work forces, control work processes, and manage, store, retrieve, manipulate, and process key web data elements.
- maintain and, as required, expand existing web pages upon government need.
- develop interactive solutions that integrate with back-end legacy systems and databases with web optimization, when directed. These work products shall comply with established DoD/AF/AFMC standards regarding web development.
- perform Microsoft .NET web development, Hypertext Markup Language (HTML and/or HTML5), Cascading Style Sheets (CSS and/or CSS3), Extensible Markup Language (XML), Ajax, C #, Visual Basic code, Entity, Model View Controller (MVC), JSON, SQL Server Reporting Services, IIS, Bootstrap, Backbone, Web Service, REST Services, SSIS, Angular JS, and Structured Query Language (SQL and/or T-SQL) within the Microsoft.NET environment.
- create and implement Web Services, data access and data manipulation techniques in the Microsoft.Net environment.
- develop applications using the Microsoft Office Web Components.

1.3.5 Content Management

The contractor shall:

- format content using text editors and electronic content management software to create, update, obtain, verify, format, convert, organize, and manage hyperlinks in various content.
- use Microsoft Office Suite for working with documents, spreadsheets, presentations, and structured/non-structured data.
- work with data format conversion techniques required to change content from one format to another.

1.3.6 Software Engineering

The contractor shall provide a Senior Software Engineer (SSE) who will provide support and technical expertise for the development of an enterprise-wide system architecture. The SSE shall perform as the technical lead for development of solutions for engineering studies and internet/intranet applications, systems engineering, systems integration, software engineering, architectural design, structured analysis, and object-oriented principles and tool suites. The SSE shall perform all phases of software development with emphasis on analysis, coding, testing, documentation, acceptance and maintenance/sustainment phases. The SSE shall define and

analyze system requirements, develop design specifications, translate specifications into programming logic, test and debug software, correct any deficiencies prior to implementation, and determine user-training requirements. The contractor shall design, document, and develop automated data structure(s) to fulfill client requirements. The SSE shall work with the Government Program Manager and contract Program/Project Manager to identify and implement the management tools, business practices, and Hazcom/eSSWB software needed to improve and maintain “on time” deliveries to the 75 ABW/SC and OO-ALC/SE customers.

1.3.7 Application Functionality Testing and Vulnerability Mitigation

The Contractor shall perform application functionality user acceptance testing to verify software and external interface functionality. Vulnerabilities identified during code security scans shall be mitigated IAW 75 ABW/SC processes and security policies prior to deployment.

1.3.7.1 Application Information Security

The Contractor shall ensure that all system or application deliverables meet the requirements of DoD and AF Information Assurance (IA) policy. Furthermore, the Contractor shall ensure that personnel performing IA activities obtain, and remain current with, required technical and/or management certifications.

The Contractor shall ensure all application code meets information systems security requirements as defined by regulation and policy in AFI 33-200 dated 18 Oct 2016. The Contractor shall protect system information and resources according to established security policies and procedures and ensure application code is updated with the latest security patches to minimize security vulnerabilities. The Contractor shall provide documentation and confirm that application code changes comply with the DoD system security policy and are properly certified and accredited in accordance with DODI 8510.01; Risk Management Framework (RMF) for DOD IT, signed 12 Mar 2014. More consistent with established disciplines and best practices for effective systems engineering, systems security engineering, and program protection planning outlined in DoDI 5000.02. The Contractor shall provide documentation as requested to support RMF Certification and Accreditation processes. When applicable, the 75 ABW/SC will review all RMF documentation for possible non-security impact approval. The Contractor shall implement procedural countermeasures and Government-issued technical advisories including STIGs, Notices to Airmen (NOTAM), Time Compliance Network Order (TCNO), Field Engineering Notices (FEN), System Advisory Notices, Heads Up Messages (HUM), Air Force Computer Emergency Response Team (AFCERT) notices, Time Compliance Technical Order (TCTO), Information Condition Changes (INFOCON), service packs and security patches according to AFCERT or Automated System Security Incident Support Team (ASSIST) guidance within the timeframe specified by the technical advisory when such notices directly apply to the application software code used or developed in HazCom/eSSWB. The Contractor shall report monthly completion of all Government-issued technical advisories as described in this paragraph to the COR (see AFI 17-100 for further information). (CDRL A011)

For those solutions that will be deployed to Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or similar environments, and thus inherit existing network security controls, application security assurance is required at the Application layer of the TCP/IP DoD Model. The Contractor shall ensure that all application deliverables adhere to Public Law 111-383,

which states the general need for software assurance. Specifically, the contractor shall ensure that all application deliverables comply with the Defense Information Systems Agency (DISA) Application Security & Development Security Technical Implementation Guide (STIG), which includes the need for source code scanning, the DISA Database STIG, as applicable to application development and a Web Penetration Test to mitigate vulnerabilities associated with SQL injections, cross-site scripting and buffer overflows. The contractor shall also support activities and meet the requirements of DoDI 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling, in order to achieve standardized, PKI-supported capabilities for biometrics, digital signatures, encryption, identification and authentication.

1.3.8 Systems Architecture

The contractor shall perform system design and architecture as it relates to areas of hardware, software, and communications; including cost/benefit analysis, data formats, and communications using heterogeneous platforms and technologies. The contractor shall maintain expertise, as defined in Appendix A, in system architecture of SQL Server and .Net application implementation and strategic vision. The contractor shall maintain “Reach-Back” capability to Microsoft problem resolution resources. The contractor shall analyze business requirements and design architectures to support HazCom/eSSWB mission needs. Contractor shall administer assigned database(s) ensuring efficiency and increasing productivity while maintaining accuracy and timeliness.

1.3.9 Configuration Management

The contractor shall adhere to established software development standards and guidelines as prescribed by a minimum level 3 Capability Maturity Model (CMM), a minimum level 3 Capability Maturity Model Integration (CMMI), Institute of Electrical and Electronics Engineers (IEEE), and International Organization for Standardization (ISO). The contractor shall follow applicable 75 ABW/SC Configuration and Change Management policies developed in accordance with CMMI, IEEE and ISO; including creating and managing the project software, and managing baseline libraries (CDRL A006).

The contractor shall develop, test and integrate software utilizing CMMI or equivalent practices, processes and services. The contractor shall maintain and track the status of each requirement using ISMT, or authorized alternate tool, through release, updating software baselines after reviews and/or testing and releasing updated baselines to the field.

The contractor shall create/update/maintain release packages including the System Release Transmittal Letter (SRTL) in accordance with 75 ABW/SC Configuration Management policies and procedures. The contractor shall perform or participate in periodic and scheduled audits of the software baselines to verify that they conform to the documentation that defines them. The contractor will use the standard 75 ABW/SC source code repository (currently using Subversion for Java products and Team Foundation Server [TFS] for Microsoft products) for source code management. The contractor shall also provide notification of implemented changes to the initiator of the change request/problem report and to the users of the system.

1.3.10 Resource Management

The Contractor shall have in place a Human Resource Management Program to ensure qualified candidates are identified, screened, placed, monitored, and trained/retained to fulfill service requirements. The Contractor shall accomplish task order by employing and utilizing qualified personnel with appropriate combinations of education, experience, knowledge, training, abilities and skills, as well as physical capabilities. The Contractor shall maintain clear organizational authority and responsibility to effectively manage and control personnel. This shall be accomplished without requiring Government employees to engage in the contractor's operational or human resource management processes.

The Contractor shall establish and provide all reasonable means to ensure that performance of this contract in a Government facility is fully complementary with, and does not run counter to, any written local operating procedure or policies that may be provided by the Government. This is consistent with the contractor's exclusive right and authority to supervise and control its employees.

1.3.11 Program Management

The contractor shall provide a Program/Project Manager (PM) to act as first-line Point of Contact for official communication with the Government and contract support. The contractor PM shall delegate work assignments to contractors and manage information flow between Government and the contract employees. This position is responsible for establishing and implementing work standards and processes and shall be responsible to address customer concerns or complaints and take timely action to resolve them. This position shall provide monthly status reports of task progress and completion. The reports shall cover monthly project activities, developmental results, projected schedule of projects, risk identification/ mitigation, and the progress toward individual project milestones (CDRL A007). Ultimately, this position shall be responsible for overall contract performance and customer satisfaction.

1.3.11.1 Program Records

The contractor shall maintain program records, such as preparation, update, coordination, and maintaining system, user, and process documentation. The contractor shall provide support to OO-ALC/SE project personnel to meet their process and documentation needs in accordance with organizational policies and standards. The contractor shall provide support in the development of templates for all required process support documentation including charts and reports as required.

1.3.11.2 Technical Support

The contractor shall provide application technical support for users at multiple locations while maintaining customer focus to elicit and define problems. The contractor shall add, delete, and modify user account information; reset passwords; answer technical queries/reports; be responsible for documenting the system configuration; troubleshoot and resolve any reported problems; provide application performance tuning. The contractor shall provide functional assistance; and provide any reporting or query requirements to the program manager. The contractor shall monitor and identify sources and trends of application and/or technical problems and recommend measures to program manager that would minimize or eliminate future

reoccurrence. The contractor shall provide Hazcom/eSSWB application support for users both internally and at remote sites. The contractor shall consult with users and technical and functional people to help determine and resolve hardware and software problems. The contractor shall provide tech support to application users and customer follow-up.

1.3.11.3 Additional Responsibilities

The program manager is responsible for interfacing with the customer. The contractor is responsible to ensure that periodic changes to safety and occupational health information delivery systems are completed within customer specifications.

1.4 Document Requirements

The contractor shall create/maintain/update the requirements in the performance of this PWS as indicated in Appendix D of this PWS.

1.4.1 User's Guide

The user guide is a technical communication document intended to give assistance to people using a particular system. It contains both a written guide and the associated images, including screenshots of how the program should appear. The contractor shall create/maintain/update the user's guide to include all modifications/upgrades impacting the user experience (CDRL A005).

1.4.2 Test Evaluation Master Plan (TEMP)/Test Cases

The contractor shall create and maintain a TEMP. A TEMP identifies the tasks and activities to be performed so that all aspects of the system are adequately tested and the system can be successfully implemented. It documents the scope, content, methodology, sequence, management of, and responsibilities for test activities, including development, system, Customer Acceptance Test, and security. The TEMP provides guidance for the management of test activities, including organization, relationships, and responsibilities.

The contractor shall ensure that tests at each level include the verification of access control and system standards, data security, functionality, and error processing. The validation process ensures that the system conforms to the functional requirements and that the system is not adversely affected. The contractor shall ensure that the TEMP is up to date and complete.

The contractor shall also create test cases/scripts/procedures and a Test Report for each block release (CDRL A004). The contractor shall update the report at each level of testing to record the results of testing and certify readiness for system implementation. The contractor shall track problems, deficiencies, modifications, and refinements identified during testing or implementation, shall be tracked under configuration control (via ISMT or authorized alternate tool), and tested using the same test procedures as those described in the TEMP.

1.4.3 Source Code

The contractor shall use the standard 75 ABW/SC source code repository (currently using Subversion for Java products and Team Foundation Server [TFS] for Microsoft products) for source code management. All source code remains the property of the government. All source code shall be developed utilizing 100% government funds and the government shall have

unlimited rights to all source code developed. Any source code that is not developed using 100% government funds shall be proposed to the contracting officer and evaluated and shall be approved by the government prior to any development activities. All source code shall be maintained in the 75 ABW/SC source code repository. Upon completion of all source code updates, the contractor shall return the source code to the repository (CDRL A001). All source code written will be the property of the United States Air Force. Under no circumstances shall any contractors retain in whole or part any amount of source code. The contractor shall surrender all source code and complete documentation to the government whenever a request is made. The contractor shall take steps to ensure that the code is retained on government property and is not removed. The contractor shall ensure that all employees are aware of this requirement.

1.4.4 System Release Packages

The contractor shall create, update, and maintain release packages for each block release, including the Software Release Transmittal Letter (SRTL) in accordance with 75 ABW/SC Configuration Management policies and procedures. The SRTL shall be provided to the Government two weeks prior to the scheduled implementation date to ensure release approval is received from 75 ABW/SC Software Review Board (CDRL A008).

2.0 SERVICE DELIVERY SUMMARY (SDS)

All surveillance observations will be recorded by the Contracting Officer’s Representative (COR).

Performance Objective	PWS Paragraph	Performance Threshold	Method of Surveillance
Administer assigned database(s) ensuring efficiency and increasing productivity	1.3.3, 1.3.6, 1.3.7, 1.3.8	Maintain 90% accuracy and timeliness.	Periodic (Quarterly)
Design, document, and develop automated data structure(s) to fulfill client requirements	1.3.2, 1.3.4	Maintain 90% accuracy and timeliness	Periodic (Quarterly)
Contractor shall provide sound information technology security service.	1.3.7.3	Maintain 100% compliance of IT security within DoD/AF Information Assurance policies.	Random
Maintain client network system IAW governing policies/mandates	1.3.6	Maintain at least 95% system availability.	Random
Work, with limited direction, stays on schedule, on cost, and in scope typically responsible for independently defining approach to tasks and solutions to problems	1.3.11, 1.3.11.1, 1.3.11.2, 1.3.11.3	Meet all government performance, schedule and cost requirements with 95% compliance.	Periodic (Monthly)
Analysis, design, development and maintenance tasks shall be completed on time in	1.3.6, 1.3.11.1, 1.3.11.2	90% of all analysis design, development and maintenance tasks shall be completed on time in accordance with approved project schedule. The remaining 10% shall be	Periodic (Quarterly)

accordance with approved project schedule		rescheduled according to Government contracting officer directions.	
Contractor shall provide Monthly Status Report.	1.3.11	Delivered on or before the 1st business day of each month No later than the 5 th day of the month with zero deviations/inconsistencies. (CDRL A007).	Periodic (Monthly)
The contractor shall provide all CDRLs accurately and on time.	Appendix D	90% on time and accurate upon submission to the government, 100% on time and accurate within 15 days of government notification of inaccuracies.	Within 30 days of report/data submittal.

3.0 GOVERNMENT FURNISHED PROPERTY

3.1 General

The government will provide contractor personnel with use of workspace, furniture, and computer equipment within Hill AFB. The contractor shall supply all office supplies. The contractor shall safeguard government property provided. At the close of each work period, government facilities, property, and materials shall be secured. The contractor shall conform to the provisions of Hill Air Force Base Instructions for safeguarding the government furnished facilities and material contained therein. The contractor shall develop and establish procedures for securing facilities provided.

All documentation provided as part of this contract shall remain government property and shall be returned to the government at the end of the period of performance. The contract point of contact (POC)/Contracting Officer's Representative (COR) will periodically inspect and inventory government property in relation to this PWS, and provide information and results to the Contracting Officer.

The PM will provide access to either the Hill AFB Local Area Network (LAN) or the use of the internet from Hill AFB, or Hill AFB email services. Government personnel will assist in the accomplishment of said service and will forward any contractor's request to the appropriate government organization. Government furnished instrumentation, hardware, or software may also be provided to the contractor as required. The contractor shall obtain approval from the government PM to use facilities, equipment, or services not identified elsewhere in the contract.

4.0 GENERAL INFORMATION

4.1 Transition Period/Orientation

Up To 30 days

The contractor shall ensure a seamless transition. The contractor's transition plan shall demonstrate how personnel, materials and equipment will be utilized through the orientation period and a method to ensure performance and to include phase-in timelines. The plan shall also include the number and position titles of personnel to be on site for the orientation period.

4.2 Phase In/Out

4.2.1 Phase In: It is anticipated that the services required for this contract may overlap with services being provided on existing contracts at 75 ABW/SC. The successful offeror shall coordinate activities with any outgoing contractors to ensure a smooth transition of services.

4.2.2 Phase Out: If there is a change in contractor or if the operation reverts to in-house, the incumbent contractor will provide familiarization, to the government or the follow-on contractor, whichever the case may be, to permit an orderly change over.

4.2.3 Software Transition Plan: The Software Transition Plan (STrP) identifies the hardware, software, and other resources needed for life cycle support of deliverable software and describes the developer's plans for transitioning deliverable items to the support agency. The contractor shall provide a software transition plan for transferring life cycle support of the deliverable to the support agency (CDRL A009).

4.3 Travel Requirements

The contractor may be required to travel to support the objectives of this PWS. The contractor shall obtain approval from the government Program Manager before traveling in support of this PWS. Airfare and per diem for travel shall be billed IAW Joint Travel Regulations (JTR). The contractor is responsible for making all necessary travel and billeting arrangements. Travel will be dictated by mission requirements in support of the customer as directed by the government PM.

4.4 Security Requirements

4.4.1 Information Assurance (IA) Technical Considerations

Network access is a privilege that may be extended to contractor employees. It may be granted only after all criteria have been met and may be suspended for cause as defined in AFMANs 17-1201 and 17-1301. Network access will be approved IAW AFMAN 17-1201, AFMAN 17-1301, AFI 16-1406, AFI 17-100, AFI 17-130, AFMAN 17-1303 and DoD 8570-01. Every individual who has access to the Air Force network (af.mil) domain, specialized systems and mission systems is a network user. Every AF network user must possess a completed and favorable National Agency Check (NAC) or an interim network access waiver package. Any costs associated with obtaining the NAC shall be the responsibility of the Contractor. Contractor will require administration rights for HazCom servers and application. Non-Classified Internet Protocol Router (NIPR) client administrative rights are not required.

4.4.2 Access to Hill AFB

4.4.2.1 The security manager shall complete a "Request for Identification Credential (AFMC Form 496)" for each employee of the contractor requiring access to Hill AFB. The requests shall be submitted to Pass and Registration (South or West Gate Visitors Center).

4.4.2.2 The contracting officer's representative (COR) will complete an "Unescorted Entry Authorization Certificate (AF Form 2586)" for each employee requiring entry into controlled areas. The request shall be submitted to Pass and Registration (South or West Gate Visitors

Center). The Contractor shall request restricted area badges for employees according to HAFBI 31-101, Installation Security Program.

4.4.2.3 The Contractor shall be required to obtain a Common Access Card (CAC). The Contractor's Program Manager will ensure completion of DD Form 1172 for each on-site employee. Each employee must then take the DD Form 1172 to 75 MSS (Military Personnel Flight) located in Building 430 to receive their CAC. The Government will provide appropriate identification cards, which shall be issued, displayed, and surrendered as directed in HAFBI 31-101, Installation Security Program. The Contractor Program Manager shall ensure that all employees have the proper identification credentials prior to entering Hill AFB. The CAC shall be worn in plain sight at all times unless it is being used to access network systems. Contractor employees shall fulfill all mandatory safety and security training required for work on a government installation.

4.5 Access to the Base Network

Network access is a privilege that may be extended to contractor employees. It may be granted only after all criteria have been met and may be suspended for cause as defined in AFI 17-100 (formerly AFI 33-115, Vol. 2). Network access will be approved IAW AFI 16-1406, AFI 17-100, AFI 17-130, AFMANs 33-223/33-285, AFSSI 5027, and DoD 5200.40. Per AFI 33-115V2, "every individual who has access to the Air Force network (af.mil) domain, specialized systems and mission systems is a network user." Every AF network user must possess a completed and favorable National Agency Check (NAC) or an interim network access waiver package. Any costs associated with obtaining the NAC shall be the responsibility of the Contractor. Contractor will require administration rights for TSS servers and application. Non-Classified Internet Protocol Router (NIPR) client administrative rights are not required.

4.5.1 The Contractor shall meet the same security requirements as government employees for access to HAFB's network or Automated Information Systems (AIS).

4.5.2 Contractor personnel performing system administration will be required to obtain and maintain a Security + Certification at task order award and through the duration of the task order. All Contractor personnel must meet the terms of this PWS and must be a United States citizen. Applicable directives include DOD 5200.2 and AFI 31-501. Any costs associated with obtaining the certification shall be the responsibility of the contractor. Additionally, a secret clearance may also be required to work in certain facilities on Hill AFB. Contractor personnel identified to work in one these facilities will be required to obtain and maintain a secret clearance while working in one of these facilities. The responsibility and costs associated with submitting and obtaining these contractor investigations and clearances shall be incumbent on the government activity in accordance with Defense Security Service message dated 29 Jul 15, Investigations for Other than Access to Classified Information (<http://www.dss.mil/>). Commanders have the authority to grant contractors interim security clearances until the final security clearance is granted in accordance with AFI 31-501, Personnel Security Program Management.

4.6 Physical Security

The contractor shall be responsible for safeguarding all government property provided for contractor use. At the close of each work period, government facilities, property, and materials shall be secured as required.

4.6.1 Key Control. The contractor shall establish and implement methods of ensuring that all keys and key cards issued to the contractor by the government are not lost or misplaced and are not used by unauthorized persons. (NOTE: ALL REFERENCES TO KEYS ALSO INCLUDE KEY CARDS. NO KEYS ISSUED TO THE CONTRACTOR BY THE GOVERNMENT SHALL BE DUPLICATED. THE CONTRACTOR SHALL DEVELOP PROCEDURES COVERING KEY CONTROL THAT SHALL BE INCLUDED IN THE QUALITY CONTROL PLAN. SUCH PROCEDURES SHALL INCLUDE TURN-IN OF ANY ISSUED KEYS BY PERSONNEL WHO NO LONGER REQUIRE ACCESS TO LOCKED AREAS).

4.6.2 The contractor shall immediately report the occurrences of a lost or duplicated key and/or access card to the contracting officer and the building monitor or facility manager who is responsible for the security of that facility.

4.6.3 In the event keys, other than master keys, are lost or duplicated, the contractor shall, upon written direction of the contracting officer, rekey or replace the affected lock or locks; however, the government, at its option, may replace the affected lock or locks or perform rekeying. When the replacement of locks or rekeying is performed by the government, the total cost of rekeying or the replacement of the lock or locks shall be deducted from the monthly payment due 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 the contractor.

4.6.4 The contractor shall prohibit the use of keys issued by the government by any persons other than the contractor's employees. The contractor shall prohibit the opening of locked areas by contractor employees to permit entrance of persons other than contractor's employees engaged in the performance of assigned work in those areas, or personnel authorized entrance by the Contracting Officer.

4.7 Non-Disclosure

The Contractor shall not divulge any information about files, data, processing activities or functions, user ID's, passwords, or other knowledge that may be gained, to anyone who is not authorized to have access to such information. The Contractor personnel shall abide by all agency rules, procedures, and standards of conduct. The Contractor personnel shall be in compliance with the Federal Information Processing Standards (FIPS) 201 Personal Identity Verification (PIV) of Contractor Employees. The Contractor shall comply with agency personal identity verification procedures identified in the contract that implement Homeland Security Presidential Directive-12 (HSPD-12), Office of Management and Budget (OMB) guidance M-05-24, and Federal Information Processing Standards Publication (FIPS PUB) Number 201. The Contractor shall insert this clause in all subcontracts when the sub-Contractor is required to have physical access to a federally-controlled facility or access to a Federal information system. If the

Contracting Officer determines that a non-disclosure agreement is required from the contractor or any of its employees, the contractor agrees to cooperate fully and without delay to execute the disclosure. The government is not obliged to accept performance from the contractor or any of its employees who decline to sign or otherwise fail to execute a non-disclosure agreement as requested by the Contracting Officer.

4.8 Quality and Safety

4.8.1 Installation-Specific Safety and Health Standards

4.8.1.1 Hill AFB, along with the entire Air Force, has adopted the Voluntary Protection Program (VPP) as recognized by OSHA. Consequently, VPP affects all “applicable contractors” operating on Air Force Installations. It is the contractor’s responsibility to ensure its employees and managers have a comprehensive understanding of VPP as well as full compliance with OSHA requirements. Detailed information on VPP is available on the OSHA website (<http://www.osha.gov/dcsp/vpp/index.html>). Contractors, whether regularly involved in routine site operations or engaged in temporary projects such as construction or repair, must follow the safety and health rules of the installation or VPP site.

4.8.1.2 Contractor shall participate in various Government initiated activities such as Continuous Process Improvement initiatives, process identification and management, various meetings, safety programs related to work center hazards/Voluntary Protection Program (VPP) and similar activities as requested by the Government.

4.8.1.3 Contractors are required to provide from their OSHA 300 information the Total Case Incident Rate/Days Away Restricted or Transferred (TCIR/DART) rates by 15 January of each year to the government PM/base safety office for submission as part of the installation’s annual OSHA Voluntary Protection Program (VPP) self-evaluation report.

4.9 Quality Control

In compliance with the clauses entitled “Inspection of Services”, 52.246 series of clauses, the contractor shall establish a complete quality control program to ensure the requirements of this contract are provided as specified. The Quality Control Program shall be documented and provided to the government for acceptance upon issuance of the contract. The basic agreement has specific areas of concern for quality control. The Services Summary Section applicable to the basic agreement may differ from the contract, and the quality control program and document will be required at the contract level. The Contracting Officer (CO) shall notify the contractor of acceptance or required modifications to the plan 15 work days after receipt of the Contractor Quality Control Plan. The contractor shall make appropriate modifications (at no additional costs to the government) and obtain acceptance of the plan by the CO within 30 days of contract award. Requirements of the plan will be outlined in the contract.

The plan shall reflect the contractor’s overall approach, internal management controls, processes, and procedures for reporting to the Government on identified aspects of quality issues. The plan shall identify the means by which the contractor will ensure quality effectiveness and demonstrate comprehensive management and review of data. The plan shall describe what is

measured, how often it is tracked and provided, who reviews and assures that appropriate action is initiated when trends are unfavorable, who the Government will contact for contractor quality issues, what method and process is used to track and resolve issues, where reports are sent and maintained, and how often quality issues are reviewed and reported. The plan shall identify how the contractor identifies and resolves deficiencies, identifies potential improvements, and maintains and makes available to the Government, documentation reflecting quality control inspections and any corrective actions taken. The Contractor shall provide copies of all discrepancies to the COR.

The Contractor's Quality Control Program assures that work complies with the requirement of the contract. This plan will be reviewed for compliance by the Program Manager and COR. The Contractor shall make appropriate corrections and modifications to the plan and obtain acceptance of the plan by the Contracting Officer before the start of the first operational performance period. Updates shall be provided whenever there is a change (CDRL A010).

4.10 Quality Assurance

The government will periodically evaluate the contractor's performance to ensure services are received. The government representative will evaluate the contractor's performance through intermittent on-site inspections of the contractor's quality control program and receipt of complaints from base personnel. The government may inspect each task as completed or increase the number of quality control inspections if deemed appropriate because of repeated failures discovered during quality control inspections or because of repeated customer complaints. Likewise, the government may decrease the number of quality control inspections if merited by performance. The government will also investigate complaints received from various customers located on the installation. The contractor shall be responsible for initially validating customer complaints. However, the government representative shall make final determination of the validity of customer complaint(s) in cases of disagreement with customer(s) and provide for resolution.

4.11 Contracting Officer's Representative (COR)

4.11.1 The COR is a representative(s) of the contracting officer and will participate in the administration of this contract. Subsequent to contract award, the identity of the COR(s), with a brief list of their duties and authority will be promptly furnished to the successful bidder/offeror.

4.11.2 The COR(s) or alternate(s) will inform the contractor when discrepancies occur and will request corrective action. The COR(s) or alternate(s) will make a notation of the discrepancy on their tally/surveillance report with the date and time the discrepancy was noted and will request the contractor to initial the entry on the report.

4.11.3 Any matter concerning a change to the scope, price, terms or conditions of this contract shall be referred to the Contracting Officer and not to the COR(s).

4.11.4 The services to be performed by the contractor during the period of this contract at all times and places shall be subject to review by the Contracting Officer or authorized representative(s).

4.12 Hours of Operation

The contractor shall perform the services required under this contract during normal business hours or after hours as may be necessary so that access to the systems may not be interrupted during normal business hours. The normal business hours window is between 6:00 AM and 6:00 PM MST, Monday through Friday, except for Federal holidays (New Year's Day, Martin Luther King Day, Presidents Day, Memorial Day, July 4th, Labor Day, Columbus Day, Veterans Day, Thanksgiving and Christmas). The contractor will be expected at work on all other days and will provide development services at offsite locations if they are unable to enter closed government facilities.

Billable hours are limited to the performance of services as defined in the TO. Government surveillance of contractor performance is required to give reasonable assurance that efficient methods and effective cost controls are being used. Work in excess of the standard 40-hour workweek requires prior written approval by the COR/QAP.

4.12.1 Emergency Services. On occasion, services may be required to support network security actions, an activation or exercise of contingency plans outside the normal duty hours described above.

4.13 Conservation of Utilities

When working at Hill AFB, the contractor shall be responsible for operating under conditions that prevent the waste of utilities. The contractor shall instruct employees in utilities conservation practices. This includes following the Normal Conservation Actions stipulated by Hill AFB and posted in that facility. The contractor shall be responsible for operating under conditions that prevent the waste of utilities, which include the following:

- Lights shall be used only in areas where and when work is actually being performed.
- Mechanical equipment controls for heating, ventilation, and air conditioning systems shall not be adjusted by the contractor or by contractor employees unless authorized.
- Water faucets or valves shall be turned off after the required use has been accomplished.
- Government telephones shall be used only for official government business.

Government telephones, computer equipment, printers and e-mail shall be used only for official government business and authorized purposes.

4.14 Government Observations

Government personnel, other than COs and COR/s may from time-to-time, with CO coordination, observe contractor operations. However, these personnel may not interfere with contractor performance.

4.15 Safety Requirements

In performing work under this contract, the contractor shall conform to the safety requirements contained in the Appendix C for all activities related to the accomplishment of the work. The contractor shall take additional immediate precautions as the contracting officer may reasonably require for safety and mishap prevention purposes.

4.16 Publications

Compliance with all publications, regulations, and operating instructions provided by the government is required when:

- a. These procedures pertain to the materials expedited herein and where the contractor is authorized by the PWS to accomplish the work specified in the publication, regulation or operating instructions.
- b. The publications prescribe USAF policies, use of materials, procedures, and processes applicable to the work requirements.
- c. The contractor is required to acquire and work on the latest version of the publication(s).

4.17 Freedom of Information Act (FOIA)/Privacy Act

All official Government records affected by this contract are subject to the provisions of the FOIA and Privacy Act. Any request received by the Contractor for access/release of information from these records to the public (including Government/Contractor employees acting as private citizens), whether oral or in writing, shall be immediately brought to the attention of the CO for forwarding to the Base FOIA Manager to ensure proper processing and compliance with the Act.

4.18 Operational Security (OPSEC)

All contractors, subcontractors, their employees, associates, and consultants who have access to critical information must comply with Air Force Instruction (AFI) 10-701, Operations Security (OPSEC), and applicable local guidance. OPSEC is a systematic means of identifying and protecting information that an adversary could use against the interests of the US. The Critical Information List (CIL) identifies sensitive information that requires protection. Counter-Measures (CM), sometimes called OPSEC Measures (OM), are control standards with which all personnel must comply in order to protect critical information.

Responsibilities:

The 75 ABW/SC must provide/approve OPSEC training curriculum for use by the contractor. Training will provide the CIL that must be protected by all personnel, listings of OPSEC measures that must be used by all personnel to protect critical information, and current foreign intelligence and industrial espionage threats, as applicable. The contractor must ensure all personnel working on the contract or having access to critical information attend initial and annually recurring refresher training and that the approved curriculum is presented. Training must be provided before personnel are allowed access to critical information. All personnel must comply with OPSEC standards and practices as trained. Additional training may be required based on updates to critical information, OPSEC measures, intelligence threat, or other fundamental changes to the OPSEC program.

The contractor must track OPSEC training statistics to include total number of personnel with access to critical information, a list of their names, when each individual received the required OPSEC training, and when annual refresher training is due. Training statistics must be forwarded the 75 ABW/SCPL OPSEC Manager quarterly. Training must be provided before personnel are allowed access to critical information. The contractor must ensure all personnel comply with OPSEC standards and practices as trained. Training may require modifications based on updates to critical information, CM/OM, intelligence threat, or other fundamental changes to the OPSEC program.

Prior to seeking approval through Hill AFB Public Affairs, any information to be released outside of official U.S. Government channels, via any media, must be coordinated through an OPSEC review. All personnel must promptly report OPSEC related incidents, issues, and concerns.

APPENDICES:

Appendix A - Hazcom/eSSWB Required Level of Expertise

Contract Project/Program Manager:

1. Program/Project Management
2. Bachelor Degree in Computer Science, Engineering or Information Systems
3. At least 5 years of experience in direct supervision over projects involving IT software development and sustainment
4. Good communication skills; oral and written

Software Engineer(s):

1. Communication skills; oral and written
2. CompTia Security + Certification
3. Bachelor's Degree in Computer Science, Engineering or Information Systems
4. Minimum of five years of experience including:
 - a. .Net or MVC framework
 - b. SQL or T-SQL
 - c. HTML and/or HTML5
 - d. CSS and/or CSS3
 - e. XML
 - f. VB and/or C#
 - g. Javascript library experience
 - h. Bootstrap, Backbone, or other responsive framework
 - i. Web development
 - j. Microsoft SQL Server
 - k. Software Validation and Testing
 - l. Technical Writing
 - m. Systems Architect
 - n. Business Process Engineering
 - o. Configuration Management

Software Developer(s):

1. Bachelor's Degree in Computer Science/Information Systems and 1 year of experience.
2. Possess an understanding of or have some familiarity with:
 - a. .Net or MVC framework
 - b. SQL or T-SQL
 - c. HTML and/or HTML5
 - d. CSS and/or CSS3
 - e. XML
 - f. VB and/or C#
 - g. Javascript library experience
 - h. Bootstrap, Backbone, or other responsive framework
 - i. Web development
 - j. Microsoft SQL Server
 - k. Software Validation and Testing
 - l. Technical Writing
 - m. Systems Architect
 - n. Business Process Engineering
 - o. Configuration Management

Server and Database Administrator(s)

1. Bachelor's Degree in Computer Science, Engineering or Information Systems
2. CompTia Security + Certification
3. Minimum of two years of experience including:
 - a. Windows server platforms
 - b. Designing, implementing, managing enterprise level database
 - c. Design data distributions and archiving solutions
 - d. Produce entity relationship and data flow diagrams

Appendix B – Mandatory Guidance and Policy

- AFI 17-100 Air Force IT Service Management
- DoD 8570.1 Information Assurance Workforce Improvement Program, Chapters 3-4 and Appendix 3 and 4
- AFI 17-130, Cyber Security Program Management
- Air Force Concept of Operations
- DoDI 8510.01, Risk Management Framework (RMF) FOR DoD Information Technology (IT)
- DoDI 5200.2, Personnel Security Program
- DoDI 8500.2, Information Assurance (IA) Implementation

Appendix C – Safety Management Plan

**SAFETY, FIRE PROTECTION AND HEALTH
SPECIFICATION
INDUSTRIAL SAFETY REQUIREMENTS**

**OGDEN AIR LOGISTICS COMPLEX
UNITED STATES AIR FORCE
HILL AIR FORCE BASE, UTAH 84056**

Hazardous Communication/Electronic Site Safety Workbook

13 Feb 2017
OO-ALC/SE
Control Number: TH170204

SECTION I - GENERAL REQUIREMENTS

A. Safety Program Requirements.

The contractor will implement a safety program that ensures protection of Government personnel and property. The program will consist of, as a minimum:

1. Mishap reporting, as defined in paragraph B1 below.
2. Routine and recurring surveillance to ensure the safety requirements of this contract are enforced.
3. Identification of segregated work site locations for operations that cannot be co-mingled with general industrial operations and the process for ACO approval of operations and changes at these specific sites.
4. All contractor personnel shall be trained and qualified to perform their duties safely.
5. The contractor shall include a clause in all subcontracts requiring the subcontractors to comply with the safety provisions of this contract, as applicable.
6. Per AFPAM 91-210, para 6.4, due to non-hazardous nature of work, a Safety Plan and corresponding site specific checklist is not required.

B. Mishap Notification

1. The contractor shall notify OO-ALC/SE or the Hill AFB Command Post after normal duty hours, and the designated Government Representative (GR), i.e., the ACO, PCO, or DCMA COR (Contracting Officer's Representative) within one (1) hour of all mishaps or incidents at or exceeding \$2,000 (material + labor) in damage to DOD property entrusted by this contract, even if the government is wholly or partially reimbursed. This notification requirement shall also include physiological mishaps/incidents. A written or email copy of the mishap/incident notification shall be sent within three calendar days to the GR, who will forward it to OO-ALC/SE. For information not available at the time of initial notification, the contractor shall provide the remaining information no later than 20 calendar days after the mishap, unless extended by the ACO.

Mishap notifications shall contain, as a minimum, the following information:

- (a) Contract, Contract Number, Name and Title of Person(s) Reporting
- (b) Date, Time and exact location of accident/incident
- (c) Brief Narrative of accident/incident (Events leading to accident/incident)
- (d) Cause of accident/incident, if known
- (e) Estimated cost of accident/incident (material and labor to repair/replace)
- (f) Nomenclature of equipment and personnel involved in accident/incident
- (g) Corrective actions (taken or proposed)
- (h) Other pertinent information

2. The contractor shall cooperate with any and all government mishap investigations. Additionally if requested by government personnel or designated government representative (GR), i.e., the ACO, PCO, or DCMA COR (Contract Officers Representative), the contractor shall immediately secure the mishap scene/damaged property and impound pertinent maintenance and training records, until released by safety investigators.
3. The contractor shall provide copies of contractor data related to mishaps, such as contractor analyses, test reports, summaries of investigations, etc. as necessary to support the government investigation.
4. The contractor shall support and comply with the safety investigation and reporting requirements of AFI 91-204, Chapters 1 – 5.

C. General Safety Requirements:

The contractor is solely responsible for compliance with all federal, state and local laws, the Occupational Safety and Health Act (OSHA) (Public Law 91-596) and the resulting standards, **OSHA Standards 29 CFR 1910 and 1926**, as applicable, and the protection of their employees. Additionally, the contractor is responsible for the safety and health of all subcontractor employees. All documents required as a result of OSHA 29 CFR 1910 and 1926 regulations, (i.e. certifications, training, respiratory protection program, workplace hazard assessments), shall be made available to the COR upon request.

The contractor shall ensure assigned personnel are adequately trained and qualified for the task being performed. Brief all personnel on the hazards involved with operations and applicable precautions to be taken. Should unidentified hazards arise, cease operations until actions are taken to eliminate or mitigate hazards to safe levels.

Contractor personnel must receive Explosive Safety Awareness Training if their duties require entry into the Explosive Clear Zone. This training will be provided by the OO-ALC Safety Office.

A Risk Assessment will be required prior to any work being accomplished, if munitions will remain in the facility.

Compliance with OSHA and other applicable laws and regulations for the protection of contractor employees is exclusively the obligation of the contractor. **Note:** The government shall assume no liability or responsibility for the contractor's compliance or non-compliance with such requirements. The contractor shall furnish to each of his/her employees a place of employment, which is free from recognized hazards. The contractor shall brief his/her employees on the safety requirements of this contract and on hazards associated with prescribed tasks. The contractor is responsible for compliance with OSHA Public Law and the resultant standards identified within. In addition, the contractor is required to flow down the safety requirements/specification to all subcontractors. This applies to Federal Acquisition Regulation (FAR) 12 commercial acquisitions as well. This contract shall in no way require persons to work in surroundings or under working conditions which are unsafe or dangerous to their health. The contractor must coordinate and perform work so as not to impact the safety of government employees or cause damage to government property. This requires providing personnel with protective equipment and associated safety equipment as may be necessary. The contractor must also protect personnel from hazards generated by the work. If the contractor employs BILINGUAL speaking employees, they must post bilingual signs and have written procedures for specific tasks in applicable languages.

SECTION II – SPECIFIC REQUIREMENTS

PEDESTRIAN CROSSWALKS: All contractor personnel are required to use the closest crosswalk, or traffic controlled intersection when crossing the road. Pedestrians must look both ways to ensure the coast is clear before stepping out into the crosswalk. Pedestrians **DO NOT** have the right of way unless they are already in the crosswalk. Contractor vehicle operators have

the same responsibilities as pedestrians, to share the road and mutually observe and yield to pedestrians.

MOTOR VEHICLES: Contractor shall comply with the standards in: DoD Directive 5525.4, *Enforcement of State Traffic Laws on DoD Installations*", Nov 2, 1981, Para 3-4; DODI 6055.4, *DoD Traffic Safety Program*, 20 Jul 99; AFI 91-207, *USAF Traffic Safety Program*, 22 May 07; and AFI 91-207 AFMC SUP1, *The US Air Force Traffic Safety Program*, 1 Oct 07. Each applies to all persons at any time on an Air Force Installation and includes all leased, owned, or privatized property including housing areas. In addition: AFI 13-213, Airfield Management, applies to all contractors, sub-contractors, vendors, commercial delivery companies, and all other private business vehicles who operate anywhere on Hill Air Force Base, including the airfield (to include the industrial areas and any buildings or hangars located upon the airfield) in support of their mission.

HOUSEKEEPING: Housekeeping shall be conducted according to the requirements in OSHA Standard 29 CFR 1910.141. *CLEAN AS YOU GO* will be enforced.

Element/Requirement	Referenced Benchmark
Contract Safety	AFPAM 91-210 Para. 6
Mishap Notification/Reporting	Appendix C, Section I AFI 91-204 Para. 4.9
Facility Fire Protection	NFPA 13, 70, & 72 NFPA 409/410 AFI 91-203 Chapters 6, 22
Handling, Storage and use of Flammable/	NFPA 30, 33
Hazardous Material Management	AFI 32-7086 HAFBSUP 1
Storage and Materials Handling	DoDI 4140.62

Appendix D - CDRLs

CDRL	Category	Item	PWS Para Reference
A001	Software Application Media	Computer Software Product	1.4.3
A002	Configuration Management	Information System Management Tool (ISMT) Authorized Autherized Tool	1.3.2
A003	Configuration Management	Database Management	1.3.3
A004	Software Documentation	Software Test Report (STR)	1.4.2
A005	Software Documentation	User Guide	1.4.1
A006	Configuration Management	Engineering Change Proposal (ECP)	1.3.9
A007	Project Management	Contractor's Monthly Status Report	1.3.11
A008	Software Documentation	Software Release Transmittal Letter	1.4.4
A009	Phase In/Phase Out	The Software Transition Plan (STrP)	4.2.3
A010	Quality Control	Quality Control Program Plan	4.9
A011	Information Security	Application Information Security	1.3.7.1

Appendix E - Acronyms

<u>Acronym/Abbreviation</u>	<u>Definition</u>
AF	Air Force
AFB	Air Force Base
AFMC	Air Force Material Command
ALC	Air Logistics Command
CCB	Configuration Control Board
CFR	Code Federal Regulation
CMM	Capability Maturity Model
CMMI	Capability Maturity Model Integration
CO	Contracting Officer
COR	Contracting Officer's Representative
CSS	Cascading Style Sheets
DEPT	Department
DoD	Department of Defense
EAI	Enterprise Application Integration
EPA	Environmental Protection Agency
eSSWB	Electronic Site Safety Workbook
FAR	Federal Acquisition Regulation
GCSS	Global Combat Support Systems
GR	Government Representative
HAFB	Hill AFB
HTML	Hypertext Markup Language
IAW	In Accordance With
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
OSHA	Occupational Safety & Health Administration
PBSA	Performance Based Service Acquisition
PEG	Potential Exposure Group
PM	Program Manager
PWS	Performance-Based Work Statement
QA	Quality Assurance
QCP	Quality Control Program
SDS	Service Delivery Summary
SS	Services Summary
SRTL	Software Release Transmittal Letter
HazCom	Hazardous Communication
USAF	United States Air Force
XML	Extensible Markup Language