STATEMENT OF WORK

CONTRACT:
DATE: 26 January 2009

TITLE: National Continuity Programs (NCP)
Software Engineering and Technical Support

1.0 SCOPE.

1.1 This is a performance-based service acquisition to provide software engineering, software testing, software integration, the development of plans, processes, guides, and procedures in support of the mission, training, lifecycle maintenance, procurement, installation, help desk services, and management support. This effort is designed to support planning, and capabilities assessment of all levels of government and the private sector.

This effort includes program management support, system engineering, requirements definition, system design, software engineering, integration, testing, system support, help desk services and life cycle maintenance of the Federal Emergency Management Agency (FEMA) National Continuity Programs (NCP) software.

This effort also provides for system engineering, software development, security architecture design, security service development and integration, to facilitate access to service and agency data sources, modules and methodologies that are essential to meeting the objectives of FEMA NCP. This effort will result in a product that will provide FEMA NCP with the IT architectural foundation for NCP software development necessary for the planning, managing and capability assessment activities of continuity and readiness.

2.0 INTRODUCTION.

2.0.1 The National Strategy for Homeland Security clearly articulates the requirement for resilience for our assets, systems and networks, but also an operational resilience to maintain comprehensive continuity programs. FEMA is responsible for ensuring that resiliency and endurance for critical systems such as the RRS, IP Locator, IVS, and other efforts required contained in NSPD-51/ HSPD-20 as amended is being designed with resilience built into the core of the enterprise system.

This Statement of Work (SOW) applies to FEMA's NSPD-51/ HSPD-20 as amended mission support and includes development/testing of information technology systems, and development of plans, processes, guides, procedures, and policies. This SOW provides the capabilities FEMA requires. The efforts described herein are services to support the development of the RRS, IP Locator, IVS and any additional software efforts in accordance with NSPD-51/ HSPD-20 as amended, and the National Continuity Policy. FEMA NCP anticipates issuing detailed tasking via task orders in the areas described below.

2.1 Background.

2.1.1 On May 9, 2007, President Bush issued National Security Presidential Directive-51/ Homeland Security Presidential Directive-20 (NSPD-51/ HSPD-20 as amended), National Continuity Policy, which established a comprehensive national policy on the continuity of Federal Government structures and operations. In this policy, the President designated the Assistant to the President for Homeland Security and Counterterrorism (APHS/CT) as the National Continuity Coordinator (NCC) and directed the NCC to lead the development of a National Continuity Policy Implementation Plan (NCPIP) that should include performance metrics by which to measure continuity readiness.

President Bush approved the NCPIP on September 27, 2007. This plan builds upon the National Continuity Policy and provides guidance to Executive Branch department and agencies on appropriately identifying and carrying out their Primary Mission Essential Functions (PMEFs) that support the eight National Essential Functions (NEFs). In this plan, the President directed the NCC to coordinate with FEMA in developing a Continuity Assessment Tool (CAT) within 90 days for the departments and agencies to measure continuity readiness against requirements contained in NSPD-51/ HSPD-20 as amended. The NCPIP further states that "FEMA will develop, operate, and maintain a continuity Readiness Reporting System (RRS) which will measure and report both the individual and aggregate ability of departments and agencies to continue their PMEFs in support of the required NEFs." The RRS will identify near real-time Continuity of Operations (COOP) and Continuity of Government (COG) programmatic capabilities and will require monthly (or as required) data input from the departments and agencies. The CAT will eventually be incorporated into the RRS to provide an automated, standardized reporting capability for all the executive branch departments and agencies.

In addition, FEMA is responsible for designing, developing, implementing and maintaining all critical continuity systems for the client agency in accordance with NSPD-51/ HSPD-20 as amended October 21, 2008.

2.1.2 Applicable Documents. In the event of a conflict between the text of this Statement of Work and the references cited herein, the text of this Statement of Work shall take precedence. Nothing in the document however, shall supersede applicable laws and regulations, unless a specific exemption has been obtained.

Authorities and References

- The National Security Act of 1947 (50 U.S.C. § 404), July 1947.
- Homeland Security Act of 2002 (6 U.S.C. § 101 et seq.).
- Federal Civil Defense Act of 1950 is *Public Law 920, 81st Congress (64 Stat. 1245).*
- Executive Order 12148, Federal Emergency Management, July 1979, as amended.
- Executive Order 13286, Establishing the Office of Homeland Security, February 28, 2003.
- Homeland Security Presidential Directive 7, Critical Infrastructure Identification,

Prioritization, and Protection, December 17, 2003.

- Homeland Security Presidential Directive 5, Management of Domestic Incidents, February 28, 2003.
- Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004.
- Presidential Decision Directive 62, Protection against Unconventional Threats to the Homeland and Americans Overseas, May 22, 1998.
- Executive Order 12656 - Assignment of National Security and Emergency Preparedness responsibilities – November 1988, as amended.
- Executive Order 12472 – Assignment of National Security and Emergency Preparedness Telecommunications Functions – April 1984, as amended.
- National Security Presidential Directive 51/Homeland Security Presidential Directive – 20 (NSPD-51/HSPD-20) – National Security Continuity Policy – May 4, 2007, as amended on October 21, 2008.
- National Communications System Directive 3-10, Minimum Requirements for Continuity Communications Capabilities, July 2007.
- Homeland Security Council – National Continuity Policy Implementation Plan- August 2007.
- Federal Continuity Directive 1 (FCD 1) – Federal Executive Branch National Continuity Program and Requirement - February 2008.
- Federal Continuity Directive 2 (FCD 2) – Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification and Submission Process – February 2008.
- GAO Report, Performance Measurement and Evaluation, May 2005.
- Central Intelligence Directive 6/3 “Protecting Sensitive Compartmented Information within Information Systems,” dated 5 June 1999.
- Section 3541 of title 44, United States Code, “Federal Information Security Management Act of 2002” (FISMA).
- Department of Defense Directive 8100.1, Global Information Grid (GIG) Overarching Policy,” September 19, 2002.
- Department of Defense Directive 8500.1, “Information Assurance (IA), “October 24, 2002.
- Department of Defense Information Assurance Certification and Accreditation Process (DIACAP), 6 July 2006 (replacement for DITSCAP).
-

National Security Agency

- NSA SR1-9, CDS Certification Test & Evaluation (CT&E) Handbook, version 3.2.1, Sept 2005.
- NSA CDS Security Test and Evaluation (ST&E) Guide, version 2.0, Feb 2006.

Other

- Institute of Electrical and Electronics Engineers/Electronic Industries Association

(IEEE/EIA) Standard 12207 (replacement for MIL-STD-498, cancelled May 1998).

3.0 TECHNICAL REQUIREMENTS. The contractor shall provide systems engineering and analysis, integration, network engineering, systems maintenance, testing, training, implementation, hardware/software installation, lifecycle management, and documentation to support FEMA NCP readiness programs.

Two major components of the FEMA NCP program suite include the Readiness Reporting System (RRS) and IPL (Internet Protocol Locator). Other systems and subsystems developed to enhance RRS and IPL capabilities, or provide additional functionality beyond RRS and IPL expanding the breadth of continuity of government programs, are described briefly below.

3.1 Readiness Reporting System (RRS). The Readiness Reporting System (RRS) tracks the continuity readiness of the Federal Executive Branch (FEB) departments and agencies (D/As). The RRS does this by collecting and storing the necessary data to provide: A continuity program status and event response status, National Essential Functions (NEFs) / Primary Mission Essential Functions (PMEFs) status for each D/A, identify trends in continuity status, identify linkages and interdependencies of the NEFs / PMEFs to the D/As, support NEF scenario-dependent driven analysis and scoring, provide for itinerary tracking of D/A officials, and report on Government Operating Status (Office of Personnel Management) and Continuity of Government Condition (COGCON) for the COOP/COG Homeland Security Advisory System. Elements of a viable continuity capability include:

- Program Plans and Procedures
- Budget
- Essential Functions
- Acquisition of Resources
- Orders of Succession
- Delegation of Authority
- Continuity Facilities
- Continuity Communications
- Vital Records Management
- Human Capital
- Test, Training and Exercise Program
- Devolution of Control and Direction
- Reconstitution Operations
- Implementation

Integral factors that must be incorporated into each of these Elements include Risk Management and Budgeting.

A Human Capital Management system will be implemented to support an effective continuity plan and program. This system will provide guidance to continuity personnel on individual preparedness measures they should take to ensure response to a continuity event, implement processes to communicate the agency's operating status to all staff, and implement process to

contact and account for all staff in the event of an emergency. Personnel (or teams) with specific skill sets will be tracked for particular mission essential functions. The system will also track other key personnel who support the PMEFs.

A Facilities Management system will be pre-populated with facilities data from the FEMA Operations Center database. It will track devolution of facilities, provide geo-mapping to locate facilities, and include data for: space available, type of equipment on hand, number of personnel that can be housed, and days of sustainability.

3.1.1 State, Local, Territorial, and Tribal Governments, and the Private Sector. The NEFs can not be performed without the robust involvement of non-Federal Government (NFG) entities and the private sector. There is an integral role that State, local, territorial, and tribal governments play in determining the needs of the public and in ensuring the essential functions (e.g. police and fire services, emergency medical care, road construction, public education) continues on a daily basis. The Federal Government's COOP, COG, and ECG plans and operations shall be appropriately integrated with the emergency and continuity plans and capabilities of State, local, territorial, and tribal governments, and private sector owners and operators of critical infrastructure, as appropriate, in order to promote interoperability and prevent redundancies and conflicting lines of authority.

A system will be implemented to coordinate with regional entities, State, local, territorial, and tribal governments, and private sector owners and operators of the Nation's critical infrastructure and key resources (CI/KR) as appropriate, and to build relationships and ensure unity of effort between these entities, as appropriate.

- Incorporate their capabilities into the agency's continuity planning and exercise activities to the maximum extent possible
- Identify hazards relevant to the agency's mission and location
- Partner with these entities to develop continuity plans that are coordinated with Federal plans to the maximum extent possible
- Participate in continuity working groups (CWGs), information sharing, training, and exercises
- Coordinate occupant emergency plans (OEPs), shelter-in-place plans, and regional and local evacuation plans
- Participate in existing alert and notification networks and credentialing initiatives
- Identify interdependencies and ensuring resiliency with critical infrastructure and services at all levels
- Coordinate continuity resource and security requirements
- Work with organizations such as DHS/Federal Emergency Management Agency (FEMA) Regional/State-level CWGs, DHS/Office of Infrastructure Protection, and the various CI/KR Sector Coordinating Councils (SCCs) and Government Coordinating Councils (GCCs), Federal Executive Boards (FEBs) and Federal Executive Associations (FEAs) to augment and strengthen coordination efforts
- Participating in other coordinating activities

3.2 Internet Protocol Locator (IPL). The Internet Protocol Locator (IPL) provides the capability to track and locate key officials at all times. IPL provides an automated capability dedicated to receiving, aggregating and distributing travel itineraries, and local residence information documents that provide detailed location and contact information for key officials. The future of IPL will provide the capability to send, receive, process and display images, and other multimedia information during deployments or contingency operations, which includes the ability to "push/pull" data to/from external interfaces.

A real-time tracking system will be incorporated into IPL to identify the location of key officials. The data may be provided by Location Based Services (LBS) available from cellular phones or other GPS devices. LBS may also be used for sending alerts and other important messages. Real-time tracking could also be used in RRS for the location and notification of D/A personnel.

To provide a graphical display of key official location, a location management system to process the positioning and GIS data on behalf of the LBS application will be incorporated into IPL. The location management system acts as a gateway and mediator between the positioning equipment and LBS infrastructure. Data provided by real-time tracking will be compared to the itinerary entered into IPL to ensure timeliness and quality of the data stored in IPL.

Biometric technologies will be incorporated into IPL for the positive identification of key officials and users. Public Key Infrastructure (PKI) will also be used for system authentication.

3.3 Test, Training, and Exercise (TT&E). A Test, Training, and Exercise (TT&E) system will assess the D/As ability to prepare and validate their organization's capabilities and programs to perform their NEFs and PMEFs during an emergency. The system will require the identification, training, and preparedness of personnel capable of performing their continuity responsibilities and the implementation of procedures to support the continuation of agency essential functions. The TT&E program should be part of a multiyear plan that addresses continuity requirements, resources to support TT&E activities, and a TT&E planning calendar. The system should be able to manage individual D/A Continuity training objectives and training plans, display required action plan for deficiencies observed during TT&E activities, and allow D/As to conduct internal training on continuity of Operations and refresher training within the system. There will be a tie between D/A continuity self assessments with Observed Performance (exercises, inspections, and actual event executions).

3.4 Situational Awareness Display. An over-arching Situational Awareness Display or Common Operating Picture (COP) system may be implemented as part of FEMA NCP suite of continuity programs. This system will pull data from other FEMA NCP systems, e.g. RRS, IPL, and real-time tracking, and in a single display, present the relevant operational information (e.g. position and status), along with other data (weather, airport location) that may influence planning and operations. Data exchanged and displayed in the COP and application program will depend on the user's credentials and security enclave, and may depend on using Service

Oriented Architecture (SOA) to control access and queries.

3. 5 Technologies Insertions - Current and Future technologies/requirements for insertion into FEMA systems include the following:

- Cellular Capability - The integration of cellular capability, to include both terrestrial and satellite based systems, which support the input and report mission, shall not be precluded in the initial design effort. Every effort shall be made to plan for the addition of this future technology insertion in subsequent spiral development efforts.

- Satellite Capability - Embedded Global Positioning System (GPS) chipset capability within the IPL hardware architecture shall not be precluded in the initial design effort. Every effort shall be made to plan for the addition of this future technology insertion in subsequent spiral development efforts.

- Global Positioning System (GPS) Capability - The addition of GPS tracking devices which directly support the IPL input capability shall not be precluded in the initial design effort. Every effort shall be made to plan for the addition of this future technology insertion in subsequent spiral development efforts.

- Voice and Data Encryption Devices - The addition of voice and data encryption devices in addition to those in the IOC design plan shall not be precluded in the initial design effort. Every effort shall be made to plan for the addition of this future technology insertion in subsequent spiral development efforts.

- Pager Capability - The ability to provide automated paging interface capabilities, to include remote activation based on customer agency identified requirements shall not be precluded in the initial design effort. Every effort shall be made to plan for the addition of this future technology insertion in subsequent spiral development efforts.

- Last Mile Blue Force Tracking Device - The ability to integrate last mile blue force tracking devices and capabilities shall not be precluded in the initial design effort. Every effort shall be made to plan for the addition of this future technology insertion in subsequent spiral development efforts.

- Biometric Authentication - The implementation of biometric authentication technologies shall not be precluded in the initial design effort. Every effort shall be made to plan for the addition of this future technology insertion in subsequent spiral development efforts.

- Public Key Infrastructure (PKI) - The use of PKI for authentication shall not be precluded in the initial design effort. Every effort shall be made to plan for

the addition of this future technology insertion in subsequent spiral development efforts.

- Smart Card Technology - The use of Smart Card Technologies for authentication shall not be precluded in the initial design effort. Every effort shall be made to plan for the addition of this future technology insertion in subsequent spiral development efforts.

- High Frequency (HF) Radio: The use of HF Radio for continuity capabilities shall not be precluded in the initial design effort. Every effort shall be made to plan for the addition of HF Radio capabilities to ensure redundancy and/or alternate contingency capabilities. This will include digital, radio frequencies, and web services.

- Joint Tactical Radio: Is a system application to be used principally in a web based internet/NIPRNET/SIPRNET, desktop computer environment, and is not envisioned to employ radio-based communications that are subject to Joint Tactical Radio system parameters.

3.6 Software Engineering. The contractor shall define a software development approach appropriate for the computer software effort to be performed under this solicitation. This approach shall be documented in a Software Development Plan (SDP). The contractor shall follow this SDP for all computer software to be developed or maintained under this effort.

The SDP shall define the contractor's proposed life cycle model and the processes used as a part of that model. In this context, the term "life cycle model" is as defined in IEEE/EIA Std. 12207.0. The SDP shall describe the overall life cycle and shall include primary, supporting, and organizational processes based on the work content of this solicitation. In accordance with the framework defined in IEEE/EIA Std. 12207.0, the SDP shall define the processes, the activities to be performed as a part of the processes, the tasks which support the activities, and the techniques and tools to be used to perform the tasks. Because IEEE/EIA Std. 12207 does not prescribe how to accomplish the task, the contractor must provide this detailed information so FEMA NCP can assess whether the contractor's approach is viable. The level of detail shall be sufficient to define all software development processes, activities, and tasks to be conducted. Information provided must include, as a minimum, specific standard, methods, tools, actions, strategies, and responsibilities associated with development and qualification.

The Contractor shall process and implement Software Engineering Institute –Capability Maturity Model (SEI-CMM) Level-2 and/or IEEE Standard 12207 in the performance of this contract.

The Contractor shall deliver to the Government a fully integrated and tested system. The solution shall meet National Security Agency (NSA) requirements. The Government shall not issue an Interim Authority to Operate (IATO).

The system must be compliant with GIG Memorandum No. 6-8510, Department of Defense

Global Information Grid Information Assurance, CJCSI 6510.01C, April 2001, Information Assurance and Computer Network Defense, Department of Defense Instruction 8510.01, 28 Nov 2007, and Department of Defense Information Assurance Certification and Accreditation Process (DIACAP), and inherit attributes of hosting network enclave.

The system will also conform to any applicable FEMA communications security standards as well as any TEMPEST standards as jointly determined by the Government and contractor.

3.6.1 User Interface Mockups. The contractor shall develop User Interface (UI) mockups prior to actual development in order to show flow and functionality.

3.6.2 Analytical Support to Capture Planning, Management and Assessment Requirements of the NCP Systems. The contractor shall provide analytical support for the development and analysis of business rules supporting the FEMA NCP systems. For example, these business rules would be related to planning, managing and assessing capabilities/activities.

3.6.3 Technical Architecture. The contractor shall develop the system architecture for FEMA NCP which is scalable and extensible based on DHS/FEMA and DOD standards. The architecture shall provide interfaces to related systems, e.g. DHS, FEMA, State Emergency Management Agencies, DoD, etc.

3.6.4 Technical Documentation. The contractor shall provide technical documentation and user guides as requested by the Technical Representatives on the operational nature of the FEMA NCP systems as well as development integration. Specifically, the contractor shall provide user guides on the operational nature of FEMA NCP systems, as well as information for the integration of external systems.

3.7 Software Development and Integration. The contractor shall provide quick prototypes of software applications to show proof of concept. The contractor shall develop application software modules, using government approved requirements and design. The contractor shall provide modifications to software in response to government requests. The contractor shall test the software, provide test reports, and demonstrate successful operation of the developed software to the government. The contractor shall ensure that all software products comply with government requirements and that system performance meets government expectations in an operational environment. Data encryption algorithms used in the application must be on the NSA list of approved encryption/decryption methods. The contractor shall provide a user-friendly interface to add/change/delete/view/data and provide for database access controls to control user access and permissions. The contractor shall install software at operational sites selected by the government and provide hands-on training to system users. The contractor shall maintain deployed systems. The contractor shall support technical discussions, troubleshoot problem areas and take corrective actions.

3.8 Application Database Support. The contractor shall design and develop the database architecture and database system to support the FEMA NCP system. The contractor shall develop the FEMA NCP software and database capabilities with the functionality and

features outlined in the NCP Requirements Matrix. The NCP Requirements Matrix shall be expanded to include all NCP requirements, scheduled and actual "sprint version", estimated and actual cost, and other information as required by the Technical Representatives.

3.9 Network Architecture and Design Support. The contractor shall provide network and hardware analysis services and recommend network and hardware configurations that will best meet the project requirements. The network architecture will comply with DISR, DIICOE, and GIG architecture and policy. The system will inherit the attributes of the local and global network environments already in place and support these environments by providing added layers of security through access control mechanisms for log on and data manipulation. The contractor shall design and implement a server and network monitoring strategy that will alert support and FEMA NCP administrators in the event of an outage or to report on server availability and response times.

3.10 System Architecture and Design Support. The system will be designed and equipped to eliminate single-points of failure, ensuring 24x7 operation of this mission critical system. There will be two fully redundant, geographically separated, secure computer centers operated by trained staff with computers and communication equipment dedicated to the mission. Each center will contain two identical suites of hardware with each suite capable of independently supporting all operations.

3.10.1 Redundant, Replicated System at Two Separate Sites. The contractor shall develop a system architecture foundation which is scalable and extensible. The architecture must be compatible with other FEMA NCP readiness application programs allowing for future data exchange between the systems. System architecture will be designed to support multiple levels of redundancy. Each of the components of the server site architecture will be supported by redundant backups at each server location. There will be two geographically separated server locations with real-time replication/synchronization of data to allow for immediate fail-over capability and recovery. The system will support stand-alone operations when one of the server sites or communication failures precludes real-time replication/synchronization. Upon restoration of the failed component, the system will replicate/synchronize all data and resume standard dual operations.

3.10.2 Cross Domain Solution. Systems implemented in FEMA NCP may involve the transfer of data from one security enclave to another, e.g. passing data from an UNCLASSIFIED network to a SECRET network and up to TOP SECRET network. The system implemented will also notify the input user whether the input was successfully saved and updated in the data store. The contractor must demonstrate knowledge and expertise in developing appropriate system and network architectures to meet the data transfer requirements, and knowledge and expertise in developing the applicable programming code.

In consultation with FEMA NCP, any Cross Domain Solutions (CDS) implemented must meet NSA accreditation and follow other DHS, FEMA, and DoD requirements.

3.11 Technical Support during Government Installation and Testing. The Contractor shall

be required, on an as-needed basis, to provide system support during government installation and testing. At a minimum, this would include,

Hardware installation support
- Web and application servers
- Database servers
- Workstations
- Network devices and appliances

Software installation support
- Operating systems
- Web software
- Application software
- Applicable updates and patches

3.11.1 Build at JITC a Quality Assurance/Accreditation Test Bed. The contractor shall demonstrate the ability to establish the FEMA NCP continuity systems utilizing contractor developed documentation and software. This sub-task shall be accomplished by the contractor at JITC test bed facilities under the supervision of the FEMA NCP designated inspector. The inspector shall validate that all code and documentation are sufficient to support the construction of an operational system utilizing only Commercial Off-The-Shelf (COTS) hardware and software, and the contractor delivered items identified in this SOW. Any necessary modifications to contractor delivered software or documentation shall be the responsibility of the contractor and shall be delivered to the government within 10 days of identification by the FEMA designated inspector.

3.11.2 On Call Support During JITC Testing. The contractor shall provide on-call support to FEMA NCP during JITC's conduct of Functional Testing at the JITC test-bed.

3.12 Certification and Accreditation (C&A). The contractor shall develop, maintain, and support DHS and DoD Certification and Accreditation (C&A) requirements as directed by the FEMA NCP Technical Representatives. The contractor shall support the C&A process as defined in DIACAP, and as well as assist in the completion and delivery of the System Security Authorization Agreement (SSAA) for the system. The Government shall oversee the C&A process to include testing and shall be the final authority for the approval process.

The contractor shall provide a Security Officer responsible for maintaining a Security Plan which will include periodic audits of the Data Management tasks described within this section. In addition, the Security Officer shall ensure that all Information Systems Accreditation documentation is complete. This includes the following items,

- IT COOP Risk Assessment
- IT COOP Risk Mitigation Plan
- FIPS 199
- Privacy Impact Assessment (PIA)

- E-Authentication
- Security Contingency Plan
- Security Test & Evaluation Plan (ST&E)
- Security Contingency Plan Results
- ATO Letter
- Security Assessment Report
- C & A Boundary & Perimeter
- C & A Registration Form
- C & A Project Plan
- Accreditation Package

3.13 Installations and Migration. The contractor shall provide installation and migration support as defined in the Migration Plan for deployment. The installation and migration shall include detailed fielding schedules of server locations and user workstations, and shall be submitted to the government prior to Official Government Acceptance Testing (OGAT). The contractor shall be expected to provide installation and migration support to various users throughout deployment.

The contractor shall provide a detained plan for the migration of existing data and users when required (e.g. change in data structure when moving from one spiral to another). Data shall be transferred without loss or degradation from the prior system.

3.12.1 Technical Support during Primary Site Build. The contractor shall provide technical support during the establishment of the primary and backup server location. FEMA/JITC shall build the system using the delivered software and documentation. Any necessary modifications to contractor delivered software or documentation shall be the responsibility of the contractor and shall be delivered to the government within 10 days of identification by the FEMA designated inspector.

3.13.2 On Call Support during Backup Site Build. The contractor shall provide on-call technical support during the establishment of the system at the backup server location. FEMA/JITC shall build the system using the delivered software and documentation.

3.14 Training. The contractor shall develop, present, and maintain training course materials and training manuals to support the FEMA NCP programs. The contractor shall participate in administrative tasks such as scheduling classes, tracking student loading and instructor assignments, and processing payments, receipts and invoices. The contractor shall provide training to users of fielded systems. The contractor shall provide a Customer Support and Training Team that shall create and execute training plans and documentation to assist FEMA NCP users in using the NCP systems.

3.15 Help Desk and Trouble Call Support. The contractor shall provide help desk support by responding to trouble calls and providing technical and administrative information for NCP systems. Support at server sites and the replication servers shall be provided during normal working hours, 5 days a week (Monday – Friday, 0700-2300, Eastern Time). Response to

trouble calls shall be provided within 15 minutes. The contractor shall provide technical support for users during normal working hours. During periods of crisis and special events, the help desk may be manned 24 hours per day, 7 days a week. Response shall be provided via any means available but the contractor shall provide a response record logged via the FEMA email system. The help desk shall provide assistance in uploading, generating queries, and downloading information. The contractor shall provide functional user training. On a monthly basis, the contractor shall provide a list of all trouble calls by project to the FEMA NCP Technical Coordinator. The list shall consist of at a minimum, call number, description, project, support location, priority, user name/activity/phone/email, date/time of call, date/time user called back, hours spent on problem, description of problem resolution, date/time problem resolved, and status. The detailed information gathered by the help desk shall assist the FEMA NCP Technical Representatives in measuring the performance of the system.

3.16 Software Configuration Management. The contractor shall perform configuration management of the FEMA NCP systems, provide input to the program office in the facilitation of the Configuration Control Board (CCB) and provide the administrative support needed to execute CCB decisions. The contractor shall attend meetings and coordinate with commands and activities on lifecycle support. The contractor shall analyze proposed changes to baseline requirements and provide detail descriptions of implementation requirements and impacts. On a monthly basis, the contractor shall provide a list of all government approved tasks by project to the Technical Coordinator. The list shall consist of at a minimum task number, task description, task type, priority, estimated hours, actual hours, approval date, estimated start/end dates, actual completion date, and status.

3.17 Working Group Meetings. The contractor shall participate in working group meetings with managers and users to help determine requirements, implementation issues, conduct reviews, and other project related purposes. The contractor shall submit meeting minutes/trip reports documenting the results of these meetings.

3.18 Lifecycle Support. The contractor shall provide measurable performance targets (metrics) for the tasks in this SOW as requested by the government. It is anticipated that there shall be formal In Progress Reviews (IPR) held quarterly in Washington D.C. These IPRs could include the following system lifecycle reviews: System Requirements Review, System Design Review, Critical Design Review, Test Readiness Review, and Operational Test Readiness Review.

The contractor shall provide system engineering and lifecycle maintenance for FEMA NCP systems. The contractor shall participate in system requirements analysis and functional requirements definition. The contractor shall use government approved methods, processes, and tools for system requirements collection, analysis, design, development, testing, installation, integration, documentation, and management. The contractor shall initially develop a "Contractor Integrated Technical Information System Implementation Plan (CITIS-IP). The contractor shall develop, publish, and maintain schemas and data base dictionaries for the systems. The contractor shall recommend software development approaches which describe program modules, classes, objects, databases, Graphic User Interface displays and reports needed

to successfully implement the application program functional requirements. The contractor shall provide technical and analytical services in support of database development, process improvement, integration and lifecycle maintenance. The contractor shall provide high-level design of network architectures, describing hardware configurations, software capabilities, and connectivity. The contractor shall provide high-level design of application software and data interfaces. The contractor shall create and register schema at the government-approved registry. The contractor shall participate in system reviews required by the government.

3.19 Management Support. The contactor shall develop presentations, reports, point papers, and other documents in support of the FEMA NCP systems as requested by the government. The contractor shall participate in the performance of all technical analysis, assessments, research, special studies and monitoring. The contractor shall participate in technical and status review meetings. The contractor shall submit project review reports. The contractor shall establish program management processes that provide on time, within budget, quality results. Contractor program management must also ensure the smooth, effective and efficient deployment and employment of the System Implementation Team. The contractor's program management for FEMA NCP programs processes shall afford opportunities for input and oversight by the government. Program management shall incorporate risk mitigation measures. The contractor shall also provide material, software, and hardware procurement support.

3.20 Method of Surveillance.

3.21 System Documentation and Software Delivery. System documents and software delivery shall be delivered to the FEMA NCP Technical Representatives for inspection and acceptance. The contractor shall provide a formal delivery of all packaged documentation and software at the completion of each task order.

3.21.1 System Documentation. The contractor shall develop and maintain the following documents for all tasks required by this SOW and as requested by the FEMA NCP Technical Representatives,

- Operational Concept Description (OCD)
- Software Requirements Specification (SRS) (includes IRS, SSS, Use-Case Diagrams)
- Software Design Description (SDD) (includes SSDD, modeling diagrams)
- Interface Design Description (IDD)
- Database Design Description (DBDD)
- Requirements Traceability Matrix (RTM)
- Software Test Plan (STP) (includes STR)
- Software Version Description (SVD)
- Software User Manual (SUM) (includes SIOM)
- Software Center Operator Manual (SCOM)
- Disaster Recovery Plan
- Software Configuration Management Plan (SCM)
- Risk Management Plan

- Test and Evaluation Master Plan
- Training Plan
- System Security Plan (SSP)
- Information Systems Accreditation Documents
- Data Migration Plan

The documentation must be reviewed, approved, and accepted by FEMA NCP.

3.22.2 Software Delivery. Software delivery shall include the following documentation, these media and documentation generally identified as,

- Release Identification
- Release Notes
- Installation Instruction including back out instructions
- Application Modules (scripts, objects and sources)
- Inventory of Modules, in accordance with system configuration
- Media (source code shall be separated from installation modules)
- Test and verification certification as required

4.0 DELIVERABLES. All software engineering artifacts produced shall be provided to FEMA NCP Technical Representatives as requested including: architectural reviews, development plans, development software, test plans, test results and all documentation for any FEMA information technology task produced under this SOW.

4.1 Progress Reports. The contractor shall provide the following monthly reports to the FEMA NCP Technical Representatives and Technical Coordinator.

4.1.1 Monthly Status Reports. The contractor shall provide Monthly Status reports. Report format and contents shall be determined by the Technical Representatives and Technical Coordinator and shall include enclosures for Actual Summary of Hours and Actual Detailed Hours. The Actual Detail of Hours shall include but is not limited to employee names, skill levels, labor hours by project/module, rates, monthly costs, cumulative costs, and Other Direct Costs (ODC). The contractor shall provide soft copy of this report written in Microsoft Word with the Actual Summary of Hours and Actual Detailed Hours in Microsoft Excel or MS Project Suite.

4.1.1.1 Monthly Status Report. The contractor shall provide an enclosure to the Monthly Status Report of the following, with contents and format specified by the Technical Representatives:

- A list of milestones scheduled and achieved for the month.
- Delays explained.
- A graph of high-level tasks for support staff and development staff.
- Estimate of work remaining with associated financial costs.

4.1.2 Monthly Financial Status Reports. The contractor shall provide Monthly Financial Status Reports. Report format and contents shall be determined by the Technical Representatives and Technical Coordinator. The contractor shall provide soft copy of this report in Microsoft Excel.

The Monthly Financial Status Report shall contain a Spend Plan enclosure with contents, format, level of detail, and number of projected months specified by the Technical Representatives and Technical Coordinator.

The Monthly Financial Status Report shall contain a Delivery Order Summary enclosure with contents and format determined by the Technical Coordinator but at a minimum contain the contract number, delivery order number, ceiling, total hours, total labor, total subcontractor labor, total fee, total ODC, total travel, total cost adjustment, total fee adjustment, total rate adjustment, total expended, balance, and projected out of funds date for all contract delivery orders.

4.1.3 In Progress Reviews. The contractor shall provide measureable performance targets for this SOW's tasks as requested by the government. It is anticipated that there shall be formal In Progress Reviews (IPR) held quarterly in Washington DC or at a NCP FEMA designated site. These IPR's could include the following System Lifecycle Reviews: System Requirements Review, System Design Review, Critical Design Review, Test Readiness Review, and Operational Test Readiness Review.

4.1.4 Trip Reports. Trip reports for all trips made during the reporting period shall be submitted as enclosures to the monthly status report. The report shall include the traveler's name, dates of travel, departure and arrival locations, purpose of trip, person visited/contacted, project, and cost information.

4.1.5 Administrative Coordination. The contractor shall use e-mail for administrative coordination issues. CLASSIFIED (up to SECRET) information can be transmitted via SIPRNET e-mail.

4.1.6 Work Completion Report. The contractor shall provide a Work Completion Report at the end of every delivery order as required by the Technical Representatives. The report format and contents shall be determined by the government but should include as a minimum, a description of all work completed (include delivery dates for deliverables); a summary of overall cost expenditures (to the module level); and any conclusions, recommendations, and proposals. The contractor shall amend the cost expenditures in a timely manner if they change.

4.2 Task Reports. The contractor shall submit a spend plan prior to initiation of any tasks.
The contractor shall submit a written status report to the Technical Coordinator and Technical Representative, submitted no later than the 15th day of the month following the reporting period, containing the minimum information of: task number, task description, estimated start/end dates, actual completion date, and status (work accomplished, description of any problems that may impede performance and corrective actions, outline of work to be performed during the next

reporting period, resources expended during the reporting period and cumulatively from the start of the task).

4.33 DATA DELIVERABLES. Data deliverable shall be submitted as specified in the attached CDRL, DD1423.

5.0 Travel Requirements. Projected trips are listed in the Travel Requirements Chart and any other travel requirements shall be specified by the government as needed.

Paragraph	# Round Trips	From	To	# People	Duration Per Trip
5.1.1	3	Washington, DC	San Diego, CA	2	5 days
5.1.2	3	Washington, DC	Johnstown, PA	2	5 days
5.1.3	6	Washington, DC	JITC Facilities	2	5 days
5.1.4	8	Washington, DC	FEMA Facilities	2	5 days

6.0 OTHER.

6.1 Security. FEMA NCP shall provide the appropriate badges, passes and other access requirements needed for contractor personnel to gain access to FEMA, JITC, and other government facilities. Due to the applications and systems that will be developed and tested, the contractor staff must hold clearances at the TOP SECRET level, based on a full-field background investigation, and must be natural born United States citizens. Interim TOP SECRET clearances are not accepted by DHS.

The contractor shall be required to furnish adequately cleared personnel with a TOP SECRET clearance for installation, testing, and maintenance. The contractor shall also be required to provide adequate personnel for the duration of the deployment and migration phase of the Task Order on a 24/7 basis to ensure a fully operational system.

Contractor personnel shall adhere to FEMA, JITC, and other government site security requirements and are required to have agency escort at all times while in the test bed sites and operational facilities. FEMA and JITC reserve the right to limit the number of personnel allowed in agency owned testing sites and operational facilities.

The contractor shall require access to Communications Security (COMSEC) information and For Official Use Only (FOUO) information.

Due to the sensitivity of the FEMA NCP programs, all documents and conversations dealing with the program, whether CLASSIFIED or UNCLASSIFIED, must be pre-approved by FEMA NCP before any information can be released to contractor's personnel not assigned on the Task Order. All contractor personnel shall be indoctrinated in the DHS Chief Security Officer (CSO) Non Disclosure procedures. Contractors are required to sign a Non Disclosure Agreement,

Standard Form 312, for this specific program prior to being given any access to such information released or generated under this contract.

Constraints: Only contractors possessing a current TOP SECRET facility clearance shall be permitted to respond to this requirement. The contractor's facility shall have full SIPRNET connectivity and secure telecommunications to ensure full collaboration between on-site and off-site personnel.

All FEMA NCP program work, whether CLASSIFIED or UNCLASSIFIED, must be performed in a minimum SECRET environment.

6.2 Place of Performance. Work shall be performed at contractor facilities and government work sites. Expected government locations are FEMA and other federal facilities, JITC facilities, and other contractor sites as deemed necessary by the Government Program Manager.

All development shall be completed in a minimum SECRET CLASSIFIED environment using FEMA equipment. SECRET safeguarding capabilities (not to exceed two (2) cubic feet) shall be available at the contractor's facilities. Because of the sensitivity of the data, the contractor shall be required to have a TOP SECRET facility clearance.

6.3 Section 508 Compliance. The continuity systems developed in this SOW is for a national security system pursuant to FAR 39.204(b) and 36 CFR 1194.3(a) and is therefore a legal exception to the requirement to acquire Electronic and Information Technology (EIT) that meets the technical provisions of the Section 508 Access Board's standards.

6.4 Government Furnished Equipment (GFE) / Government Furnished Information (GFI). The contractor shall furnish all professional, technical, and clerical personnel and services, software, materials, equipment (general office) and travel to conduct the necessary work as specified in this SOW.

All computer hardware and communication infrastructure that are required to develop, support, and implement the system shall be government furnished equipment. The contractor shall maintain accountability of government material and maintain receipts, inventory, adjustments, and shipments of government property. The contractor shall periodically perform, record, and disclose physical inventory results. A physical inventory shall be performed upon contract completion or termination. The contractor shall investigate and promptly furnish a written narrative of all incidents of loss, damage, destruction, or theft to the government property administrator as soon as the facts become known or when requested by the government. The contractor shall award subcontracts that clearly identify assets to be provided and shall ensure appropriate flow down of contract terms and conditions.

6.5 Key Personnel. The contractor shall identify key contractor personnel and submit résumé's and certifications supporting such designation for the duration of the project

covered by this SOW. FEMA NCP shall have the right to review and approve the resumes of all contractor personnel selected prior to initiation of specified task(s), to include determination of eligibility for access to FEMA and JITC facilities. The contractor may propose changes or additions to the key personnel matrix, which must be approved by the Technical Representatives.

Replacement of key personnel shall require 30 days notice to the FEMA NCP Contract Officer via the Technical Representatives. A transition period of no less than one (1) week and no more than two (2) weeks is acceptable. Replacement of key personnel shall require the Technical Representative's approval.

6.6 Other Direct Charges. The Contractor shall purchase hardware and software products as directed by the FEMA NCP Technical Representatives. Items furnished shall be for the performance of contract, not consumed, and returned to the government upon contract completion. Cross Domain solutions, must be selected from current NSA approved list of baseline equipment.

6.7 Inspection and Acceptance. In accordance with this SOW, the government shall exercise its right to inspect the continuity systems prior to delivery to Official Government Acceptance Testing (OGAT). This inspection shall take place at the vendor's test lab to verify, validate, and audit all software and hardware to determine that the supplies and services conform to the delivery order requirements. This inspection shall be conducted by FEMA/DHS/NCP or its designated representative.

The contractor shall coordinate services, deliverables, and delivery schedules with Ms. Linda Grinnage and Mr. O. Vincent Brown with the understanding that all work shall be within scope of this SOW. The contractor shall submit all deliverables to Ms. Linda Grinnage and Mr. O. Vincent Brown for inspection and acceptance.

Technical Representatives:

Ms. Linda Grinnage
Department of Homeland Security
Federal Emergency Management Agency
National Continuity Programs Directorate
(202) 646-4000

Mr. O. Vincent Brown
Department of Homeland Security
Federal Emergency Management Agency
National Continuity Programs Directorate
(202) 646-3880

Technical Coordinator:
Mr. Ed Faltemier
SPAWARSYSCEN Pacific Code 5244
(808) 471-8009 x 222