

SECTION H - SPECIAL CONTRACT REQUIREMENTS

H.1 TRAINING

- (a) The Contractor shall be responsible for all education and skills-based training necessary to ensure that the employee is qualified to perform the work assigned.
- (b) The Contractor shall develop in-house orientation and training courses for new staff regarding the TSP, the work to be performed, and the associated guidelines, procedures, processes, etc. The Agency will review these materials at the request of the Contractor.

(End of Clause)

H.2 REMOVED

Removed.

(End of Clause)

H.3 REPORTING AND OTHER COMMUNICATIONS

- (a) The Contractor shall keep the Agency apprised of its activities on a regular basis. The Agency expects the Contractor to be in daily or weekly contact via phone, e-mail, or face-to-face with its Agency counterparts. The frequency of these contacts will change depending upon the workload, issues identified, etc.
- (b) The Contractor shall participate in daily operations teleconferences to provide statuses on the TSP and FRTIB systems. Teleconferences are generally less than an hour in duration. The Contractor shall provide an update on its activities any discuss any achievements, problems, or future activities that may impact the workload.
- (c) The Contractor shall provide a comprehensive calendar year end report, detailing workload, process or other enhancements.
- (d) The Contractor shall provide ad hoc performance, workload, or other reports at the request of the Agency. These requests generally arise from external requests for information or special projects requiring data other than that normally provided to the Agency during the Contractor's normal reporting activities.

(End of Clause)

H.4 INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY REQUIREMENTS FOR IT CONTRACTS

H.4.A General

- (a) For the purpose of this clause, "Contractor" shall include all Prime and Subcontractor organizations and their personnel
- (b) All Contractors shall be subject to the same Federal laws (including the Privacy Act of 1974 and FISMA), regulations, standards and FRTIB policies as FRTIB, and FRTIB personnel regarding information and information system security. Contractors must follow policies and procedures outlined in FRTIB Directive 61 "Enterprise Information Security Program and Policy Authorization," its policies, and its handbooks to ensure appropriate security controls are in place.
- (c) These security requirements shall apply to all FRTIB, TSP, and Contractor systems used to access FRTIB or TSP systems or to take custody of FRTIB or TSP data.

H.4.B Access to Agency Information and Information Systems

- (a) Contractors shall request logical (technical) and/or physical access to FRTIB information and FRTIB information systems for employees only to the extent necessary: (1) to perform the services specified in the contract, (2) to perform necessary maintenance functions for electronic storage or transmission media necessary for performance of the contract, and (3) for individuals who first satisfy the same conditions, requirements and restrictions that comparable FRTIB employees must meet in order to have access to the same type of FRTIB information.
- (b) The following are FRTIB's approved policy exceptions for meeting FRTIB's background screenings/investigative requirements for certain types of Contractors:
 - (1) Contract personnel not accessing FRTIB information resources such as personnel hired to maintain the facility grounds, construction contracts, utility system Contractors, etc.,
 - (2) Contract personnel with limited and intermittent access to equipment connected to facility networks on which no FRTIB sensitive information is available, such as Contractors who install, maintain, and repair building equipment such as fire alarm; heating, ventilation, and air conditioning equipment; elevator control systems, etc. If equipment to be repaired is located within sensitive areas (e.g. computer room/communications closets) they must be escorted while on site.

H.4.C Information Custodial Requirements

- (a) Information made available to the Contractor by FRTIB for the performance or administration of this contract or information developed by the Contractor in performance or administration of the contract is FRTIB property and shall be used only for those authorized purposes and shall not be used in any other way without the prior written agreement of the Contracting Officer. This clause expressly limits the Contractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d)(1).
- (b) FRTIB information will not be co-mingled with any other data on the Contractors/subcontractors information systems/media storage systems in order to ensure FRTIB requirements related to data protection and media sanitization can be met. FRTIB also reserves the right to conduct IT resource inspections to ensure data separation and on-site inspection of information destruction/media sanitization procedures to ensure they are in compliance with FRTIB policy requirements.
- (c) Prior to termination or completion of this contract, Contractor will not destroy information received from FRTIB or gathered or created by the Contractor in the course of performing this contract without prior written approval by the FRTIB Contracting Officer. Any data destruction done on behalf of FRTIB by a Contractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in FRTIB Directive 28A, Records Management Directive, and the Agency's Media Protection Policy.
- (d) The Contractor will receive, gather, store, back up, maintain, use, disclose and dispose of FRTIB information only in compliance with the terms of the contract and applicable Federal and FRTIB information confidentiality and security laws, regulations and policies. Applicable Federal information security regulations include Federal Information Processing Standards (FIPS) and Special Publications (SP) issued by the National Institute of Standards and Technology (NIST). If Federal or FRTIB information confidentiality and security laws, regulations and policies become applicable to the FRTIB information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies, including FIPS or SP, in this contract.
- (e) Contractors collecting, storing, or disseminating Personal Identifiable Information (PII) data must conform to all pertinent regulations, laws, and FRTIB directives related to privacy. Pursuant to its requirements under the Privacy Act and its EISRM directives, the Agency will be conducting privacy reviews and assessments on any internal or external system which has

- FRTIB or TSP data. To that end, the Agency may require 1) access to any non-FRTIB owned system with FRTIB or TSP data, 2) documentation relating to non-FRTIB owned systems, and 3) the ability to perform automated assessments of non-FRTIB owned systems.
- (f) The Contractor shall not make copies of FRTIB information except as necessary to perform the terms of the agreement or to preserve electronic information stored on Contractor electronic storage media for restoration. In case any electronic equipment or data used by the Contractor needs to be restored to an operating state.
 - (g) If FRTIB determines that the Contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for FRTIB to terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.
 - (h) Contractor will store, transport or transmit FRTIB sensitive information in an encrypted form, using a FRTIB-approved encryption application that meets the requirements of NIST's FIPS 140-2 standard.
 - (i) Except for uses and disclosures of FRTIB information authorized by this contract for performance of the contract, the Contractor may use and disclose FRTIB information only in two other situations: (i) after notifying the FRTIB, in response to a qualifying order of a court of competent jurisdiction, or (ii) with FRTIB's prior written approval. The Contractor will refer all requests for, demands for production of, or inquiries about, FRTIB information and information systems to the FRTIB Contracting Officer for response.
 - (j) Notwithstanding the provision above, the Contractor shall not release PII records protected by the Privacy Act under any circumstances, including in response to a court order, and shall immediately refer such court orders or other inquiries to the FRTIB Contracting Officer for response.
 - (k) The Contractor will not use technologies banned in FRTIB in meeting the requirements of the contract. See Attachment J.8.22, FRTIB Banned Technologies.

H.4.D Information System Design and Development

- (a) Information systems that are designed or developed for or on behalf of FRTIB at non-FRTIB facilities shall comply with all FRTIB policies developed in accordance with Federal Information Security Management Act (FISMA), NIST, and related FRTIB security and privacy control requirements for Federal information systems. This includes standards for the protection of information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline

security controls commensurate with the FIPS 199 system security categorization.

- (b) During the analysis phase of the software development cycle, a privacy impact assessment will be completed, provided to the COR, and approved by the FRTIB Privacy Officer in accordance with FRTIB Privacy Impact Assessment EISRM Directive.
- (c) The security controls must be designed, developed, approved by FRTIB, and implemented in accordance with the provisions of FRTIB security system development life cycle as outlined in NIST Special Publication 800-37 and FRTIB EISRM Directive.
- (d) The Contractor will be required to design, develop, or operate a System of Records on individuals to accomplish an Agency function subject to the Privacy Act of 1974, (as amended), Public Law 93-579, December 31, 1974 (5 U.S.C.552a) and applicable Agency regulations. Violation of the Privacy Act may involve the imposition of criminal and civil penalties. The Contractor agrees to –
 - (1) Comply with the Privacy Act of 1974 (the Act) and the Agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an Agency function when the contract specifically identifies –
 - (a) The systems of records; and
 - (b) The design, development, or operation work that the Contractor is to perform;
 - (2) Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a system of records on individuals that is subject to the Act; and,
 - (3) Include this Privacy Act clause, including this subparagraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a system of records.
- (e) In the event of violations of the Act, a civil action may be brought against the Agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an Agency function, and criminal penalties may be imposed upon the officers or employees of the Agency when the violation concerns the operation of a system of records on individuals to accomplish an Agency function. For purposes of the Act, when the contract is for the operation of a system of

records on individuals to accomplish an Agency function, the Contractor is considered to be an employee of the Agency.

- (f) Definitions for terms like system of records can be found in the Privacy Act of 1974.

H.4.E Information System Hosting, Operation, Maintenance or Use

- (a) For information systems that are hosted, operated, maintained, or used on behalf of FRTIB at non-FRTIB facilities, Contractors are fully responsible and accountable for ensuring compliance with applicable Privacy Act, FISMA, NIST, FIPS, SP, and FRTIB security and privacy directives and handbooks. The Contractor security control procedures must be identical, not equivalent, to those procedures used to secure FRTIB systems. A privacy impact assessment (PIA) must also be provided to the COR and approved by FRTIB Privacy Office prior to operational approval. All external Internet connections involving non-FRTIB information systems must be reviewed and approved by FRTIB prior to implementation.
- (b) Adequate security controls for collecting, processing, transmitting, and storing of personally identifiable information, as determined by the FRTIB Privacy Office, must be in place, tested, and approved by FRTIB prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of FRTIB. These security controls need to be stated within the PIA and supported by a risk assessment. If these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII.
- (c) Outsourcing (Contractor facility/Contractor equipment/Contractor staff) of systems or network operations, telecommunications services, or other managed services requires certification and accreditation (C&A) of the Contractor's systems in accordance with NIST Special Publication 800-37 and FRTIB EISRM Directive and a privacy impact assessment of the Contractor's systems prior to operation of the systems. FRTIB-owned (FRTIB facility/FRTIB equipment) Contractor-operated systems, third party or business partner networks require a system interconnection agreement and a memorandum of understanding (MOU) which detail what data types will be shared, who will have access, and the appropriate level of security controls for all systems connected to FRTIB networks.
- (d) The Contractor must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the FRTIB Contracting Officer and the Information System Security Officer (ISSO) for entry into FRTIB's Plan of Action and Milestone (POA&M) management process. The Contractor will use FRTIB's POA&M process to document

planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes approved by the FRTIB. Contractor procedures will be subject to periodic, unannounced assessments by FRTIB officials. The physical security aspects associated with Contractor activities will also be subject to such assessments. As updates to the system occur, an updated PIA must be submitted to the FRTIB Privacy Office through the COR for approval.

- (e) All storage media used within non-FRTIB owned information systems that is used to store, process, or access FRTIB sensitive information must have all FRTIB sensitive information removed, cleared, sanitized, or destroyed in accordance with FRTIB policies and procedures (including its Media Protection Policy) upon: (1) completion or termination of the contract or (2) disposal or return of the storage media by the Contractor or any person acting on behalf of the Contractor, whichever is earlier.

H.4.F Security Incident Investigation

- (a) The term “security incident” means an event that has, or could have, resulted in unauthorized access to, loss or damage to FRTIB assets, or sensitive information, or an action that breaches FRTIB security procedures. Even if outside regular business hours, the Contractor shall immediately (within one (1) hour of first becoming aware) notify the Contracting Officer Representative (COR) and simultaneously, the designated Information System Security Officer (ISSO) for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor has access.
- (b) To the extent known by the Contractor, the Contractor’s notice to FRTIB will identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the FRTIB information/assets were placed at risk or compromised), and any other information that the Contractor considers relevant.
- (c) The Contractor will simultaneously report the incident to the appropriate law enforcement entity(ies) of jurisdiction in instances of theft or break-in or other criminal activity. The Contractor, its employees, and its subcontractors and their employees will cooperate with FRTIB and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The Contractor will cooperate with FRTIB in any civil litigation to recover FRTIB information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to the incident.

- (d) The FRTIB shall have the right to participate in any investigation relating to a suspected or actual breach and, pursuant to such an investigation, shall have access to any and all related data including but not limited to affected files, systems, briefings, devices (including hard drives), and interim as well as final reports and analyses.
- (e) To the extent practicable, the Contractor shall mitigate any harmful effects on individuals whose FRTIB information was accessed or disclosed in a security incident. In the event of a data breach with respect to any FRTIB Sensitive Information processed or maintained by the Contractor or subcontractor under the contract, the Contractor is responsible for consequential damages to be paid to FRTIB.
- (f) Contractor shall bear the losses and expenses (including attorneys' fees) associated with a data breach, including, without limitation, any costs (1) of providing notices of a data breach to affected individuals and to applicable regulatory bodies and (2) of remedying and otherwise mitigating any potential damage or harm of the incident, including, without limitation, establishing call centers, providing credit monitoring, or credit restoration services.

H.4.G Security Controls Compliance Testing

- (a) On a periodic basis, FRTIB reserves the right to evaluate any or all of the security controls and privacy practices implemented by the Contractor under the clauses contained within the contract. With 10 working-day's notice, at the request of the FRTIB, the Contractor shall fully cooperate and assist in an FRTIB-sponsored security controls assessment at each location wherein FRTIB information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of FRTIB. The FRTIB may conduct a security control assessment on shorter notice (to include unannounced assessments) determined by FRTIB in the event of a security incident or at any other time.

H.4.H Security and Privacy Training

- (a) All Contractor employees and subcontractor employees requiring access to FRTIB information and FRTIB information systems shall complete the following before being granted access to FRTIB networks:
 - (1) Sign and acknowledge understanding of and responsibilities for compliance with the attached Rules of Behavior relating to access to FRTIB information and information systems;
 - (2) Successfully complete FRTIB Cyber Security Awareness training and annual refresher training as required;

- (3) Successfully complete FRTIB General Privacy training and annual refresher training as required; and
 - (4) Successfully complete any additional cyber security or privacy training, as required for FRTIB personnel with equivalent information system access [to be defined by the FRTIB program official and provided to the Contracting Officer for inclusion in the solicitation document – e.g., any role-based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.]
- (b) The Contractor shall provide to the Contracting Officer a copy of the training certificates or other proof of training for each applicable employee within one week of the initiation of the contract and annually thereafter, as required. It is the Contractor's responsibility to ensure the Agency is notified of new staff members who require training.
 - (c) Failure to complete this mandatory training within the timeframe required will be grounds for suspension or termination of all physical and/or electronic access privileges and removal from work on the contract until such time as the training is completed.

H.4.I Contractor Requirements, Confidentiality and Non-Disclosure

- (a) Contractor personnel will have access to some privileged and confidential materials of the FRTIB. These printed and electronic documents are for internal use only, are not to be copied or released without permission, and remain the sole property of the FRTIB. These materials are protected by the Privacy Act of 1974 (revised by PL 93-5791). Unauthorized disclosure of Privacy Act covered materials is a criminal offense.
- (b) The preliminary and final deliverables and all associated working papers, application source code, and other material which has been generated by the Contractor in the performance of this SOW are the exclusive property of the FRTIB.
- (c) The CO will be the sole authorized official to release verbally or in writing, any data, the draft deliverables, the final deliverables, or any other written or printed materials pertaining to this SOW. The Contractor shall release no information. Any request for information relating to this SOW presented to the Contractor shall be submitted to the CO for response.
- (d) The Contractor recognizes that in the performance of this contract the Contractor may receive or have access to sensitive information, including information provided on a proprietary basis by other private or public entities. The Contractor agrees to safeguard these privileges and use the information

exclusively in the performance of this contract. The Contractor shall follow all FRTIB rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations.

- (e) The Contractor shall maintain physical security in accordance with NIST, and EISRM requirements at all facilities housing the activities under this SOW, including any subcontractor facilities. The Contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to sensitive data must comply with published procedures to protect the privacy and confidentiality of such information as required by FRTIB.

H.4.J Proprietary Information Requirement

- (a) The Contractor may be required to negotiate agreements with commercial system vendors relating to non-disclosure of vendor-proprietary information. If the Contractor uses copyright or otherwise licensed software in any deliverable under this order, the Contractor must secure unlimited use rights for the Agency. In addition, the Contractor is required to pass all software licenses on to the FRTIB within 30 days after completion of the tasks.
- (b) The Contractor shall limit access to the minimum number of employees necessary for order performance for all information considered sensitive or proprietary in nature. If the Contractor is uncertain of the sensitivity of any information obtained during the order then the Contractor has a responsibility to ask the FRTIB representative.
- (c) The Contractor shall indoctrinate all personnel employed by the Contractor and any subcontractors involved in this order on their roles and responsibilities for proper handling and nondisclosure of sensitive FRTIB or proprietary information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information.

H.4.K Security: Information System Security

- (a) The Contractor shall ensure adequate LAN/Internet, data, information, and system security in accordance with FRTIB standard operating procedures and standard contract language, conditions laws, and regulations. The Contractor's firewall and web server shall meet or exceed the FRTIB minimum requirements for security. All FRTIB data shall be protected behind an approved firewall. Any security violations or attempted violations shall be reported to the FRTIB COR and the Information Security Officer as soon as possible. The Contractor shall follow all applicable FRTIB policies and

procedures governing information security, especially those that pertain to certification accreditation.

H.4.L Security Requirements for Unclassified Information Technology Resources

- (a) The Contractor and their personnel shall be subject to the same Federal laws, regulations, standards and FRTIB policies as FRTIB personnel, regarding information and information system security. These include, but are not limited to Federal Information Security Management Act (FISMA), and guidance and standards, available from the Department of Commerce's National Institute of Standards and Technology (NIST). This also includes the use of common security configurations available from NIST's Web site at: <http://checklists.nist.gov/>.
- (b) To ensure that appropriate security controls are in place, Contractors must follow the procedures set forth in the Agency's EISRM policies which are in Section J.

H.4.M Security Audits

- (a) At least once every twelve (12) months following the Contract signing date, Contractor, at its own expense, shall cause to be conducted a Statement of Standards Attestation Engagements (SSAE) 16 audit (or any successor standard) on its operations, including the operations of its affiliates and subcontractors, that are involved in the provision of the Services under this Contract. The SSAE-16 Audit shall be performed by an independent auditing firm registered and in good standing with the Public Company Accounting Oversight Board and any successor thereto. The time period covered for each annual SSAE-16 Audit shall be for October 1 through September 30. Contactor shall provide the Agency with:
 - (1) the auditor's scope, description of controls, testing results and opinion, as well as the auditor's recommendations and any required planned or completed corrective actions; complete copies of such reports; and Contractor corrective action plans (if any) with committed delivery dates related to the results of such SSAE-16 Audit. **Any failure to meet such corrective action plan shall be deemed a material breach of this Contract.**
- (b) If any SSAE-16 Audit as set forth above results in a qualified opinion, upon the first such occurrence, the Contractor shall perform such corrective plan in accordance with the committed delivery dates to successfully resolve the applicable deficiency.
- (c) **The Parties agree that such second occurrence of a SSAE-16 Audit resulting in a qualified opinion shall be deemed a material breach of this**

Contract and a default and the Agency may terminate this Contract. For the avoidance of doubt, no early termination fees shall apply in connection with such a termination.

H.4.N Personnel Security

- (a) All Contractor staff assigned to work under this Contract must be U.S. citizens or resident aliens with current valid green cards.
- (b) Contractor will not allow any of its employees to access Agency information and systems except to the extent that an employee needs access in order to facilitate work under this contract, and Contractor shall coordinate with Agency to ensure that all such individuals are screened according to the EISRM policies and standards prior to being provided access to Agency information and systems. The level of screening shall be dependent upon a risk designation assigned to this Contract and the individual's responsibilities and access required to perform services. Contractor shall ensure that all individuals on the Contract are re-screened according to the policies and standards in FRTIB's Personal Identity Verification program and EISRM program. Failure to coordinate these rescreening activities could result in individuals being denied access.
- (c) Contractor shall notify the COR and designated Agency security administration function(s) of the termination of any individual assigned to work on this Contract not more than 2 hours after termination. Contractor shall retrieve any and all credentials, property, documentation, etc. from the terminated employee. Contractor shall ensure that at all times it retains complete control of Contractor- and Agency-owned information systems and information.
- (d) Contractor shall notify the COR and designated Agency security administration function(s) of the transfer of any individual permanently assigned to work on this Contract between major Services functions not more than 2 business days after the effective date of the transfer.
- (e) Contractor shall ensure that all individuals assigned to perform Services on this Contract periodically accept and sign Non-Disclosure Agreements, Rules of Behavior, and applicable Ethics Agreements.
- (f) Contractor shall immediately (within 24 hours) revoke all system access rights and restrict security (e.g., access badges) of its personnel who are no longer employed on this contract. Contractor shall document its compliance with this requirement upon Agency request.
- (g) For Agency review, Contractor shall maintain a system of sanctions against individuals who perform Services under this Contract for failure to comply with any Contractor or Agency security requirements.

(End of Clause)

H.5 TRAVEL

- (a) The Contractor shall obtain approval from the COR prior to traveling. Airfare for travel and per diem expenses will be subject to government travel management policy and the Federal Travel Regulation, and will be reimbursable in accordance with current allowances as specified on the GSA website. The Contractor is responsible for making all necessary travel arrangements.

(End of Clause)

H.6 CONTRACT TRANSITION PERIOD AND CLOSE OUT

- (a) The Contractor recognizes that the work and services covered by this contract are vital to the FRTIB mission and must be maintained without interruption; at the commencement, at any time work is to be “returned to the Agency” (contract down-scope), and the expiration of this contract. It is therefore understood and further agreed in recognition of the above:
- (1) Upon follow-on contract award, the Contractor shall continue to perform all duties under this contract;
 - (2) Upon contract expiration or contract down-scoping, a Successor may continue to produce products and provide services.
 - (3) The Contractor agrees to exercise its commercially reasonable efforts, as defined by case law and cooperation to effect an orderly and efficient transition from the Contractor (upon contract award) and to a Successor as further described in this section.
 - (4) The Contractor shall, in conjunction with FRTIB, prepare, submit and implement a Phase-Out Plan defining activities and schedules necessary to meet contract production delivery, services, and other deliverable requirements. Coordination with the Contractor may start sooner than CO’s notification and Contractor’s support may be utilized for longer than 180 days. The Phase-Out Plan shall be submitted six months in advance of the expiration of the final Agency exercised option period, regardless of the date of CO notification to the Contractor to provide support. The Contractor shall assume full responsibility for work until assumption thereof by the Successor Contractor. Execution of the proposed Phase-Out Plan or any part thereof shall be accomplished in accordance with the Contracting Officer’s direction and approval. The Phase-Out Plan is subject to the CO’s approval, and shall:

- (A) Identify the specific work activities and supporting instruments required of both the Contractor and Successor to support the Successor's Phase-In, and the dates by which such work must be accomplished. Phase-Out Plan topics and related tasks should include items such as, but not limited to, the following:
- (i) A personnel training program and a date for transferring responsibilities for each division of work described in the Plan. All work performed by the Contractor must be included in the Phase-Out Plan.
 - (ii) Transfer/novation of licenses, permits, leases, and subcontracts; or support activities related to replacement of non-transferable instruments, including transfer of shared environments (e.g., SharePoint and contents), hardware warranties/licenses, and software licenses.
 - (iii) Review, evaluation and transition of all current support services and work processes.
 - (iv) Information regarding in-process Agency-funded work that may necessarily be transferred from the Contractor to the Successor for completion.
 - (v) Conversion of all current and historical financial and participant data as-is for processing to the successor Contractor with no retention of original or copied data by Contractor on work stations or other media.
 - (vi) Access to personnel of prime and sub-Contractor employees as permitted by law and regulation.
 - (vii) Non-interference access to operating areas, with required security clearance or waiver by FRTIB.
- (b) Upon CO's written notice, the Contractor shall execute the approved Phase-Out Plan. Specifically, the Contractor shall:
- (1) Coordinate with designated FRTIB personnel.
 - (2) Maintain and provide status information showing Phase-Out tasks, progress on each task, and expected completion dates.
 - (3) Coordinate with successor Contractor to complete Phase-Out to Phase-In tasks. FRTIB will approve completion of tasks.

- (4) Provide sufficient experienced personnel during the Phase-Out period to ensure that the services and production in this contract are realized without interruption.
 - (5) Transfer all business and/or technical documentation, including creation and transfer of gaps in documentation.
 - (6) Transfer all compiled and uncompiled source code, to include all versions, maintenance updates and patches for all file sets.
 - (7) Conduct orientation to introduce successor Contractor to TSP and Agency personnel, programs, and users to the Contractor's team, tools, methodologies, and business processes.
 - (8) Dispose of Contractor purchased/Agency owned assets, including facilities, equipment, furniture, phone lines, computer equipment, etc.
 - (9) Transfer Government Furnished Equipment (GFE) and Government Furnished Information (GFI), and GFE inventory management assistance.
 - (10) Participate in applicable Agency debriefing.
 - (11) Complete personnel out-processing procedures.
 - (12) Turn-in of all Agency keys, ID/access cards, and security codes.
- (c) The Contractor agrees to negotiate in good faith with the Agency and Successor Contractor for the timely and cost effective execution of work activities performed pursuant to this section and the associated Phase-Out Plan. Unless otherwise approved by the CO in advance, Phase-Out work performed by the Successor Contractor shall be invoiced to the Agency. Agreements between the Successor Contractor and Contractor defining the work content, terms, and conditions, shall be separate and apart from this section. The Agency will include a Phase-Out/Phase-In section in the Successor Contractor's contract requiring the Successor to act in good faith.
- (d) Phase Out costs are not to be included in the Offeror's Cost Proposal.

(End of Clause)

H.7 COMPLIANCE WITH REGULATIONS

- (a) The Contractor shall comply with all statutes, regulations, directives, instructions, and references applicable to this acquisition as required by FRTIB, including, without limitation, those specified or referred to in this contract. The Contractor and its employees shall become acquainted with and shall comply with the rules and regulations of the FRTIB's facilities, including,

but not limited to security, controlled access, personnel clearances, and conduct with respect to health and safety at the site, regardless of whether or not title to the facility is vested in the FRTIB.

NOTE: The Federal Retirement Thrift Investment Board (or Agency) is a Government Agency operating on non-appropriated funds whose mission is to act solely in the interest of the Thrift Savings Plan participants and beneficiaries. As a non-appropriated fund Agency, it is not bound by the Federal Acquisition Regulation (FAR).

(End of Clause)

H.8 NON-DISCLOSURE REQUIREMENTS

- (a) Attachment J.2 is a required Non-Disclosure Agreement and it must be completed by each Contractor (and subcontractor) employee and delivered to the CO before performing work under this contract.
- (b) Restrictions on Use, Disclosure, and Duplication of Confidential and Non-Public Information. Confidential and non-public information, for purposes of this clause is, but is not limited to, all financial, statistical, personnel and/or technical data which is furnished, produced, generated, or otherwise available to the Contractor, during the performance of this contract. Unless otherwise specified, confidential and non-public information shall not be used for purposes other than performance of work under this contract without the prior written consent of the CO. The Contractor, and its employees, agents, subcontractors, and subcontractor personnel are restricted from duplicating or disclosing confidential or non-public information, in whole or in part, outside the FRTIB for purposes other than fulfillment of the requirements set forth in this contract. Any presentation of any confidential or non-public information, or any reports or material derived from confidential or non-public information shall be subject to CO review and approval prior to publication or dissemination. Any questions about whether information is confidential or non-public shall be referred to the CO prior to use, disclosure, or duplication.
- (c) Non-Disclosure Agreement For Confidential And Non-Public Information. Section 2635.703 of title 5, Code of Federal Regulations, and the Privacy Act of 1974 (5 U.S.C. § 552a) expressly prohibit unauthorized disclosure and improper use of confidential or non-public information or documents. The Contractor, and its employees, agents, subcontractors, and subcontractor personnel who will have access to confidential or non-public information or documents in the performance of the contract, agree to be bound by Section 2635.703 of title 5, Code of Federal Regulations, and the Privacy Act of 1974 (5 U.S.C. § 552a) and the terms set forth in the attached Non-Disclosure Agreements (Attachment J2). The Contractor and all personnel assigned to the contract agree not to divulge to any unauthorized person non-public or confidential information obtained from the FRTIB in performance of their duties under the contract. Violation of this clause by the Contractor, its

employees, agents, subcontractors, or subcontractor personnel may result in termination of the contract and/or civil suits and/or criminal prosecution.

(End of Clause)

H.9 APPROVAL OF SUBCONTRACTS

- (a) The Agency reserves the right to approve or disapprove any subcontract. Therefore, the Contractor shall provide copies of subcontracts for any work required by this contract and obtain the CO’s approval of all subcontracts.

(End of Clause)

H.10 PERSONNEL

- (a) The Contractor shall provide skilled personnel required for the effective and efficient performance of this contract.
- (b) The Contractor shall designate a point of contact that is available during normal business hours and a point of contact that will be on-call during non-business hours in case of emergencies.

Name	Telephone Number

- (c) Key Personnel Qualifications.
 - Minimum qualifications for the following key personnel are:
 - 1) Program Executives and Deputy(s) shall have:
 - a Master’s degree and 10 years of directly related experience and progressively greater responsibilities, or
 - a Bachelor’s degree and 10 years in a leadership/management role and 5-7 years professional IT experience.
 - 2) Other key personnel must have a Bachelor’s degree or 8 years of directly related experience and progressively greater responsibilities.
- (d) Key Personnel. The Contractor must include in its proposal, by name and capacity, the key personnel to be assigned to perform and carry out all phases of work under this contract. The Contractor’s key personnel include the following:

Name	Capacity	Telephone Number

- (e) The individuals named above are considered key personnel and are essential for the successful completion of all work assigned under this contract. In the event any individual on the list of key personnel is to be removed or diverted from this contract, the Contractor must (1) notify the Contracting Officer; (2) supply written justification as to why the individual(s) is being removed or diverted; and, (3) provide resume of the proposed substitute or replacement including the education, work experience, etc., of each new person for Agency approval. All notifications and other information must be submitted to the Contracting Officer at least 14 calendar days in advance of the action.
- (f) The Contractor must not, under any circumstances, remove or divert key personnel unless prior written authorization has been granted by the Contracting Officer. The person replacing the key person must have the same or higher qualifications and experience as the person replaced.

(End of Clause)

H.11 CONTRACTOR RESPONSIBILITIES/STANDARDS OF CONDUCT

- (a) The FRTIB will not exercise any supervision over the Contractor's employees. The Contractor's employees, if on-site at FRTIB facilities under this contract, shall only engage in duties specified in this contract, and not in other business, or political, charitable or other duties. The Contractor shall not recruit on FRTIB premises or otherwise act to disrupt official FRTIB business. The Contractor shall be responsible for maintaining satisfactory standards of employee competency, conduct, appearance, and integrity, and shall be responsible for taking such disciplinary action with respect to its employees as may be necessary. The Contractor shall include the substance of this clause in any of its subcontracts.

(End of Clause)

H.12 CONTRACTOR CONSENT TO BACKGROUND INVESTIGATION

- (a) Contractor personnel shall be required to undergo a U.S. Government background investigation. Based on the nature of Contractor staff's tasks and access, the required level of Contractor staff's background investigation will be determined by FRTIB staff. Such a background investigation may be the equivalent of an Office of Personnel Management National Agency Check

Inquiry (NACI), Minimum Background Investigation (MBI), Background Investigation (BI), or a background investigation appropriate for matters dealing with national security, and may include, but is not limited to, an FBI fingerprint check, credit check, inquiries into current and past employers, schools attended, references, and local, state, and federal law enforcement authorities criminal records check.

- (b) All completed background investigation will be adjudicated by an FRTIB Personnel Security Officer for a Fitness Determination. If a Contractor employee receives an unfavorable fitness determination, it is the responsibility of the Contractor to provide a replacement in accordance with the contract.

NOTE: "Contractor Employee Fitness" is the level of character and conduct determined necessary for an individual to perform work for or on behalf of a Federal Agency as a Contractor employee. "Fitness determination" means a decision by an Agency that an individual has or does not have the required level of character and conduct necessary to perform work for or on behalf of a Federal Agency as a Contractor employee. A favorable fitness determination is not a decision to appoint or contract with an individual.

- (c) Contractors will be responsible for the cost associated with conducting Agency sponsored background investigations for its staff.
- (d) Contractor shall ensure their employees and those of their subcontractors have the proper credentials allowing them to work in the United States. Persons later found to be undocumented or illegal aliens will be remanded to the proper authorities.
- (e) The Contractor shall not be entitled to any compensation for delays or expenses associated with complying with the provisions of this clause. Furthermore, nothing in this clause shall excuse the Contractor from proceeding with the contract as required.

(End of Clause)

H.13 CONFIDENTIAL INFORMATION

- (a) All information received by the Contractor as a result of performance of this contract is confidential and is subject to the Privacy Act. The Contractor and Contractor personnel shall maintain this information in strict confidence and shall not disclose this information, or any information obtained as the result of its performance of this contract, to any person or entity, other than employees or bona-fide Contractors of the FRTIB, without the prior written approval of the Agency. The Contractor and Contractor personnel shall not disclose this information to any person or entity or otherwise make any improper use of this information during or after the performance period of this contract. The

Contractor and Contractor personnel shall maintain this information in strict confidence and shall make no changes to the information except as necessary in the performance of the contract. The Contractor and Contractor personnel and their successors are prohibited forever from using this information for their personal or business gain, personally or for another, directly or indirectly, without prior written approval of the Agency. This provision/clause, or a provision/clause with an identical effect, shall be placed in any subcontracts.

(End of Clause)

H.14 ADVERTISING AND RELEASING OF INFORMATION

- (a) The Contractor must not publicize or advertise in relation to this contract without the prior written approval of the Agency. Also, the Contractor may not release information or report on its performance under the contract without the prior written approval of the Agency.

(End of Clause)

H.15 CONTINGENCY RE-OPENER

- (a) Should the Agency exercise its authority to execute an in-scope modification, the FRTIB Contracting Officer and the Contractor shall re-negotiate the pricing. Prior to reaching a bi-lateral agreement, the FRTIB Contracting Officer and technical staff will evaluate the proposed pricing to ensure it is realistic and reasonable.

(End of Clause)

H.16 CONTRACTOR CODE OF BUSINESS ETHICS AND CONDUCT (6 JUNE 2012)

- (1) **Definitions** As used in this clause—

(a) “Agent” means any individual, including a director, an officer, an employee, or an independent Contractor, authorized to act on behalf of the organization.

(b) “Full cooperation”—

- (1) Means disclosure to the Agency of the information sufficient for law enforcement to identify the nature and extent of the offense and the individuals responsible for the conduct. It includes providing timely and complete response to Federal Retirement Thrift Investment Board (or Agency) auditors’ and investigators’ request for documents and access to employees with information;

- (2) Does not foreclose any Contractor rights arising in law, the FAR as applicable, or the terms of the contract. It does not require—
 - (i) A Contractor to waive its attorney-client privilege or the protections afforded by the attorney work product doctrine; or
 - (ii) Any officer, director, owner, or employee of the Contractor, including a sole proprietor, to waive his or her attorney client privilege or Fifth Amendment rights; and
- (3) Does not restrict a Contractor from—
 - (i) Conducting an internal investigation; or
 - (ii) Defending a proceeding or dispute arising under the contract or related to a potential or disclosed violation.
- (c) “Principal” means an officer, director, owner, partner, or a person having primary management or supervisory responsibilities within a business entity (*e.g.*, general manager; plant manager; head of a subsidiary, division, or business segment; and similar positions).
- (d) “Subcontract” means any contract entered into by a subcontractor to furnish supplies or services for performance of a prime contract or a subcontract.
- (e) “Subcontractor” means any supplier, distributor, vendor, or firm that furnished supplies or services to or for a prime contractor or another subcontractor.
- (f) “United States,” means the 50 States, the District of Columbia, and outlying areas.

(2) Code of business ethics and conduct

- (a) Within 30 days after contract award, unless the Contracting Officer establishes a longer time period, the Contractor shall—
 - (1) Have a written code of business ethics and conduct; and
 - (2) Make a copy of the code available to each employee engaged in performance of the contract.
- (b) The Contractor shall—
 - (1) Exercise due diligence to prevent and detect criminal conduct; and
 - (2) Otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.
- (c) The Contractor shall timely disclose, in writing, to the FRTIB Chief Risk Officer, with a copy to the Contracting Officer, whenever, in connection

with the award, performance, or closeout of this contract or any subcontract there under, the Contractor has credible evidence that a principal, employee, agent, or subcontractor of the Contractor has committed—

- (1) A violation of Federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations found in Title 18 of the United States Code; or
 - (2) A violation of the civil False Claims Act ([31 U.S.C. 3729-3733](#)).
- (d) The Agency, to the extent permitted by law and regulation, will safeguard and treat information obtained pursuant to the Contractor's disclosure as confidential where the information has been marked "confidential" or "proprietary" by the company. To the extent permitted by law and regulation, such information will not be released by the Agency to the public pursuant to a Freedom of Information Act request, 5 U.S.C. Section 552, without prior notification to the Contractor. The Agency may transfer documents provided by the Contractor to any department or Agency within the Executive Branch if the information relates to matters within the organization's jurisdiction.
- (e) If the violation relates to an order against a Government-wide acquisition contract, a multi-Agency contract, a multiple-award schedule contract such as the Federal Supply Schedule, or any other procurement instrument intended for use by multiple agencies, the Contractor shall notify the FRTIB Chief Risk Officer.

(3) Business ethics awareness and compliance program and internal control system

- (a) This paragraph (c) does not apply if the Contractor has represented itself as a small business concern pursuant to the award of this contract or if this contract is for the acquisition of a commercial item as defined at FAR 2.101. The Contractor shall establish the following within 90 days after contract award, unless the Contracting Officer establishes a longer time period:
- (b) An ongoing business ethics awareness and compliance program
- (1) This program shall include reasonable steps to communicate periodically and in a practical manner the Contractor's standards and procedures and other aspects of the

Contractor's business ethics awareness and compliance program and internal control system, by conducting effective training programs and otherwise disseminating information appropriate to an individual's respective roles and responsibilities.

- (2) The training conducted under this program shall be provided to the Contractor's principals and employees, and as appropriate, the Contractor's agents and subcontractors.
- (c) An internal control system
- (1) The Contractor's internal control system shall—
 - (i) Establish standards and procedures to facilitate timely discovery of improper conduct in connection with Agency contracts; and
 - (ii) Ensure corrective measures are promptly instituted and carried out.
 - (2) At a minimum, the Contractor's internal control system shall provide for the following:
 - (i) Assignment of responsibility at a sufficiently high level and adequate resources to ensure effectiveness of the business ethics awareness and compliance program and internal control system.
 - (ii) Reasonable efforts not to include an individual as a principal, whom due diligence would have exposed as having engaged in conduct that is in conflict with the Contractor's code of business ethics and conduct.
 - (iii) Periodic reviews of company business practices, procedures, policies, and internal controls for compliance with the Contractor's code of business ethics and conduct and the special requirements of Agency contracting, including—
 - (a) Monitoring and auditing to detect criminal conduct;
 - (b) Periodic evaluation of the effectiveness of the business ethics awareness and compliance program and internal control system, especially if criminal conduct has been detected; and
 - (c) Periodic assessment of the risk of criminal conduct, with appropriate steps to design, implement, or modify the business ethics awareness and compliance program

and the internal control system as necessary to reduce the risk of criminal conduct identified through this process.

- (3) An internal reporting mechanism, such as a hotline, which allows for anonymity or confidentiality, by which employees may report suspected instances of improper conduct, and instructions that encourage employees to make such reports.
- (4) Disciplinary action for improper conduct or for failing to take reasonable steps to prevent or detect improper conduct.
- (5) Timely disclosure, in writing, to the FRTIB Chief Risk Officer, with a copy to the Contracting Officer, whenever, in connection with the award, performance, or closeout of any Agency contract performed by the Contractor or a subcontract thereunder, the Contractor has credible evidence that a principal, employee, agent, or subcontractor of the Contractor has committed a violation of Federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations found in Title 18 U.S.C. or a violation of the civil False Claims Act (31U.S.C. 3729-3733).
 - (i) If a violation relates to more than one Agency contract, the Contractor may make the disclosure to the FRTIB Chief Risk Officer and Contracting Officer responsible for the largest dollar value contract impacted by the violation.
 - (ii) If the violation relates to an order against a Government-wide acquisition contract, a multi-Agency contract, a multiple-award schedule contract such as the Federal Supply Schedule, or any other procurement instrument intended for use by multiple agencies, the Contractor shall notify the FRTIB Chief Risk Officer and the respective agencies' Contracting Officers.
 - (iii) The disclosure requirement for an individual contract continues until at least 3 years after final payment on the contract.
 - (iv) The Agency will safeguard such disclosures in accordance with paragraph (b)(3)(ii) of this clause.
 - (v) Full cooperation with any agencies responsible for audits, investigations, or corrective actions.

(4) Subcontracts

- (a) The Contractor shall include the substance of this clause, including this paragraph (d), in subcontracts that have a value in excess of \$1,000,000 and a performance period of more than 120 days.
- (b) In altering this clause to identify the appropriate parties, all disclosures of violation of the civil False Claims Act or of Federal criminal law shall be directed to the FRTIB Chief Risk Officer, with a copy to the Contracting Officer.

(End of Clause)

H.17 LIMITATION OF AGENCY'S OBLIGATION

- (a) The Contractor will notify the Contracting Officer in writing at least ninety days prior to the date when, in the Contractor's best judgment, the work will reach the point at which the total amount payable by the Agency, including any cost for termination for convenience, will approximate 75 percent of the total amount then allotted to the contract for performance of the applicable item(s). The notification will state (1) the estimated date when that point will be reached and (2) an estimate of additional funding, if any, needed to continue performance of applicable line items up to the next scheduled date for allotment of funds, or to a mutually agreed upon substitute date. The notification will also advise the Contracting Officer of the estimated amount of additional funds that will be required for the timely performance of the item(s) funded pursuant to this clause, for a subsequent period agreed to by the parties. If after such notification additional funds are not allotted by the date identified in the Contractor's notification, or by an agreed substitute date, the Contracting Officer will terminate any item(s) for which additional funds have not been allotted, pursuant to the clause of this contract entitled "Termination for Convenience of the Government."

(End of Clause)

H.18 IDIQ TASK ORDERING AND CORE SOFTWARE CHANGE REQUEST PROCEDURES

- (a) IDIQ TASK ORDERING PROCEDURE

(1) Only the Contracting Officer may issue task orders to the Contractor, providing specific authorization or direction to perform work within the scope of the Contract and as specified in the schedule. The Contractor may incur costs under this Contract in performance of task orders and task order modifications issued in accordance with this clause. No other costs are authorized unless otherwise specified in the Contract or expressly authorized by the Contracting Officer.

(2) Prior to issuing a task order, the Contracting Officer shall provide the Contractor with the following data:

(i) A functional description of the work identifying the objectives or results desired from the contemplated task order.

NOTE: The Agency will indicate potential organizational conflict of interest when the task order is for a significant change (e.g., the replacement of a major system component), before proceeding further.

(ii) Proposed performance standards to be used as criteria for determining whether the work requirements have been met.

(iii) A request for a task plan from the Contractor to include the technical approach, period of performance, appropriate cost information, and any other information required to determine the reasonableness of the Contractor's proposal.

(3) Within **14** calendar days after receipt of the Contracting Officer's request, the Contractor shall submit a task response conforming to the request.

(4) After review and any necessary discussions, the Contracting Officer may issue a task order to the Contractor containing, as a minimum, the following:

(i) Date of the order.

(ii) Contract number and order number.

(iii) Functional description of the work identifying the objectives or results desired from the task order, including special instructions or other information necessary for performance of the task.

(iv) Performance/quality assurance standards, as required.

(v) Maximum dollar amount authorized (CPFF, T&M, or FFP).

(vi) Any other resources (travel, materials, equipment, facilities, etc.) authorized.

(vii) Delivery/performance schedule including start and end dates.

(5) The Contractor shall provide acknowledgment of receipt to the Contracting Officer within **1** calendar days after receipt of the task order.

(6) On rare occasions, if time constraints do not permit issuance of a fully defined

task order in accordance with the procedures described in paragraphs (a) through (d), a task order including a ceiling price may be issued. The task order will be definitized within 30 calendar days of the issuance of the task order.

(7) The Contracting Officer may amend tasks in the same manner in which they were issued.

(b) **CORE SOFTWARE CHANGE REQUEST (SCR) PROCEDURES**

(1) FRTIB or Contractor staff must enter core system software changes into the Task Management System (TMS) before any work is performed. TMS is used to track the initiation and disposition of a project throughout the software development life cycle.

(2) No work shall occur prior to FRTIB approval.

(End of Clause)

H.19 USE OF CONTRACTOR PERSONNEL DURING PERFORMANCE

The Agency reserves the right to utilize third-party contractors during the performance of this contract.

(End of Clause)

H.20 OPERATING LEVEL AGREEMENTS (OLA)

(a) The success of the TESS Contract is dependent on the efforts of multiple Contractors. At a minimum, the Contractor shall develop, maintain and adhere to OLAs with the following contracts and their successors:

- i. Investment Manager(s)
- ii. Annuity Vendor(s)
- iii. Call Centers
- iv. Data Entry
- v. TSP Benefits Operations
- vi. Fulfillment (Printing and Mailing)
- vii. Lockbox

The Contractor shall develop, maintain and adhere to OLA's with any other interfaces the Contractor deems necessary to avoid negatively impacting the TESS contract work.

In accordance with CDRL MGMT-07, The Contractor shall provide all OLA's to the Contracting Officer (CO) for Agency review and approval.

(b) The Contractor shall document agreements with other FRTIB Contractors

- described in (a) above via Operating Level Agreements. The Agency will not be a party in such Operating Level Agreements. All costs associated with such agreements are included in the negotiated price of this contract. In order to achieve efficient and effective implementation of TESS operations; the Contractor shall establish the means for coordination and exchange of information with other FRTIB Contractors. The information to be exchanged shall be that required by the Contractors in the execution of their respective contract requirements. The Contractors are strongly encouraged to seek out and foster cooperative efforts that will benefit TESS contract work with increased safety, efficiency, and productivity.
- (c) The Contractor is not relieved of any contract requirements or entitled to any adjustments to the contract terms because of the failure to resolve a disagreement with any of the other FRTIB Contractors. Liability for the improper disclosure of any proprietary data contained in or referenced by any agreement shall rest with the parties to the agreement, and not the Agency.
- (d) The following are high-level descriptions of the interactions we anticipate the TESS Contractor having with other FRTIB contractors working on the TSP Recordkeeping program.
- i. Investment Manager(s) – The organization that makes investments in the portfolios of securities that make up the TSP funds, in accordance with FRTIB policy, is currently BlackRock, Inc. The investment manager is responsible for all activities associated with the management of portfolios: buying and selling securities on a day-to-day basis, portfolio monitoring, settlement of transactions, performance measurement, and regulatory reporting. The interaction with the TESS Contractor, in both production and non-production environments, includes: (1) establishing and maintaining secure network connectivity, (2) operating an electronic data exchange interface, (3) responding to security and non-security incidents, (4) operations and maintenance of the AMI and CFIS applications, and (5) resolve Recordkeeping and/or pricing issues with FRTIB and the Investment Manager.
 - ii. Annuity Vendor – MetLife is responsible for the administration of annuities for TSP participants which guarantee periodic payments after the annuitant reaches retirement and requests payments. Interaction with the TESS Contractor includes: (1) establishing and maintaining secure network connectivity, (2) operating an electronic data exchange interface, (3) responding to security and non-security incidents, (4) receiving annuity payout instructions (5) payments from the TSP, (6) verification of receipt of information and payments, and (7) resolving Recordkeeping and/or annuity issues.

- iii. Call Centers - There are two remote locations, one of which is a government owned Contractor operated (GOCO) facility managed by SERCO NA, Inc.; the second is a Contractor owned Contractor operated (COCO) facility managed by Active Network. Calls to and from TSP participants are handled through the PSR application. The representatives service participants' inquiries and process transactions and through email and regular mail. The interaction with the TESS Contractor includes: (1) establishing and maintaining secure network connectivity, (2) establishing and maintaining voice network services, (3) responding to security and non-security incidents, (4) operating and maintaining the Interactive Voice Response (IVR) and PSR applications, (5) AG workflow, and (6) updating messages on IVR and PSR.
- iv. Data Entry – Currently the service provider is SunGard which is responsible for receiving, sorting, and processing mail and fax images sent to the TSP. This includes processing all participant transaction and beneficiary forms. The interaction with the TESS Contractor includes: (1) establishing and maintaining secure network connectivity, (2) establishing and maintaining fax services, (3) responding to security and non-security incidents, and (4) operating and maintaining the AG workflow, DocXP, and AnyDOC applications.
- v. TSP Benefits Operations –
 - a. Agency Technical Services (ATS), a Serco contract, interacts with more than one hundred agency payroll offices (across the Federal Government) that submit TSP participant data for several million TSP participant accounts. ATS administers diagnostic and corrective actions to resolve payroll interface data discrepancies between the Agency payroll systems and the TSP Recordkeeping systems.
 - b. The Special Processing Unit (SPU) is managed by Integrated Benefits Solution (IBS), a Serco subcontractor, and processes roll-ins, treasury credits, NSF check returns, manual notices and adjustments. Integrated Benefits Solution also handles, in conjunction with the FRTIB, any unique issues or situations not encountered in typical day-to-day operations.
 - c. Legal Processing Unit and Death Benefits Unit – Serco operates the Legal Processing Unit which handles all processing related to court orders, powers of attorney, guardianship or conservatorship orders, and the following forms: TSP-13, TSP-U-13, TSP-16, TSP-U-16, and Internal Revenue Service W4-P. Serco also operates the Death Processing Unit which is responsible for processing TSP Death Benefits Claims.

- d. The interaction between these functions and the TESS Contractor includes: (1) establishing and maintaining secure network connectivity (including external connectivity to US Treasury), (2) establishing and maintaining fax services, (3) responding to security and non-security incidents, (4) interfacing with Treasury, (5) interfacing with the Federal Reserve Bank, (6) interfacing with US Bank lockbox, (7) coordinating with the TESS Recordkeeping function and other Contractors for any manual activities resulting from adjustments or special activities, and (8) operating and maintaining the custom software CODIS and DEDIS (being replaced with CaMS), including interfaces with COTS software package, Omni and fulfillment vendors
- vi. Fulfillment (Printing and Mailing) –RR Donnelley provides print and mailing related services by generating all statements, mailings, notices, participant forms, and tax reporting forms. The interaction with the TESS Contractor in both production and non-production environments includes: (1) establishing and maintaining secure network connectivity, (2) operating an electronic data exchange interface, (3) responding to security and non-security incidents, and (4) operating and maintaining applications for the creation of statements, notices, and other participant mailings.
- vii. Lockbox –US Bank is the provider that accepts inbound payments for roll-ins, loan payments, etc. The interaction with the TESS Contractor in both production and non-production environments includes: (1) establishing and maintaining secure network connectivity, (2) operating an electronic data exchange interface, (3) responding to security and non-security incidents, (4) operating and maintaining lockbox application, and (5) coordinating with the Special Processing Unit.

(End of Clause)

H.21 CONFLICTS OF INTEREST

H.21.A General

Subpart 9.5 of the Federal Acquisition Regulation (48 C.F.R. 9.5), prescribes responsibilities, general rules, and procedures for identifying, evaluating, and resolving organizational conflicts of interest.

H.21.B Purpose

The purpose of this clause is to avoid, neutralize, or otherwise mitigate organizational conflicts of interest which might exist related to a Contractor's performance of work required by this contract. Such conflicts may arise in situations including, but not limited to: a Contractor's participation, as Offeror or representative of an Offeror, in a procurement in which it has provided

assistance in the preparation of the Agency's requirements and specifications; a Contractor providing advice and/or assistance to the Agency for a procurement in which the Contractor or an entity that the Contractor represents is an actual or potential Offeror; and a Contractor's participation, as Offeror or representative of an Offeror, in a procurement where the Contractor has obtained confidential or proprietary information relating to competing Offerors as a result of the Contractor's work on prior contracts.

H.21.C Definition

For purposes of this clause, the term "Contractor" means: The Contractor; any of the Contractor's parent companies, affiliates or other entities in which the Contractor or such parents or affiliates have a financial interest; successors in interest to the Contractor or any of its parents or affiliates; proposed consultants or subcontractors at any tier; and employees thereof.

H.21.D Restrictions

The Contractor agrees:

- (a) They shall remain ineligible to participate in any capacity (including participating as a prime Contractor, subcontractor, or as the representative of another party) in contracts, subcontracts, or quotes (whether solicited or unsolicited) that directly relate to the Contractor's performance of work under this Contract.
- (b) Prior to beginning work, to execute Confidentiality Agreements, Statements of Non-Disclosure or other documents which the CO believes are needed to protect the proprietary nature or confidentiality of information provided by the Agency or otherwise received by the Contractor in connection with work under this Contract.
- (c) Not to accept any compensation or any other form of payment from any source other than the Agency for services rendered under this Contract.
- (d) To immediately notify the CO of any offer of compensation, other form of payment, or thing of value made by any source other than the Agency to the Contractor related to services rendered under this Contract.
- (e) Prior to performing work, immediately notify the CO of any potential conflict of interest which would prevent or limit the Contractor's ability to perform the work requested.
- (f) To immediately notify the CO of any conflict of interest discovered during performance of work; provided that the CO will have the right to impose such restrictions as he/she deems appropriate on Contractor's performance, based on the existence of such a conflict or, if the CO determines that such restrictions would not adequately address the conflict of interest at issue, to terminate this contract at no cost to the Agency.
- (g) In the event, that the Contractor withholds information regarding the existence of

a conflict of interest from the Agency; the CO may terminate this contract at no cost to the Agency.

- (h) To include this Conflict of Interest clause, including this subparagraph, in all subcontracts at all tiers (appropriately modified to preserve the Agency's rights hereunder) which involve the performance of work by subcontractors (if any) in support of this contract.
- (i) In addition to the remedies stated above, that the Agency may terminate this contract for cause in the event of the Contractor's breach of any of the above restrictions.

(End of Clause)

H.22 MITIGATION OF ORGANIZATIONAL CONFLICTS OF INTEREST.

- (a) Mitigation plan. The Organizational Conflict of Interest Mitigation Plan and its obligations are hereby incorporated in the contract by reference.
- (b) Changes.
 - (1) Either the Contractor or the Agency may propose changes to the Organizational Conflict of Interest Mitigation Plan. Such changes are subject to the mutual agreement of the parties and will become effective only upon incorporating the change into the plan by contract amendment.
 - (2) In the event that the Agency and the Contractor cannot agree upon a mutually acceptable change, the Agency reserves the right to make a unilateral change to the OCI Plan as necessary, with the approval of the head of the contracting activity, subject to Contractor appeal as provided in the Disputes clause.
- (c) Violation. The Contractor shall report any violation of the Organizational Conflict of Interest Mitigation Plan, whether by its own personnel or those of the Agency or other FRTIB Contractors, to the Contracting Officer. This report shall include a description of the violation and the actions the Contractor has taken or proposes to take to mitigate and avoid repetition of the violation. After conducting such further inquiries and discussions as may be necessary, the Contracting Officer and the Contractor shall agree on appropriate corrective action, if any, or the Contracting Officer will direct corrective action.
- (d) Breach. Any breach of the above restrictions or any nondisclosure or misrepresentation of any relevant facts required regarding organizational conflicts of interests to be disclosed may result in termination of this contract for default or other remedies as may be available under law or regulation.
- (e) Subcontracts. The Contractor shall include the substance of this clause, including this paragraph (e), in subcontracts where the work includes or may include tasks related to the organizational conflict of interest. The terms

“Contractor” and “Contracting Officer” shall be appropriately modified to reflect the change in parties and to preserve the Agency’s rights.

(End of Clause)

H.23 DISCLOSURE OF ORGANIZATIONAL CONFLICT OF INTEREST AFTER CONTRACT AWARD.

- (a) If the Contractor identifies an actual or potential organizational conflict of interest that has not already been adequately disclosed and resolved (or waived in accordance with FAR 9.503), the Contractor shall make a prompt and full disclosure in writing to the Contracting Officer. This disclosure shall include a description of the action the Contractor has taken or proposes to take in order to resolve the conflict. This reporting requirement also includes subcontractors actual or potential organizational conflicts of interest not adequately disclosed and resolved prior to award.
- (b) Mitigation Plan. The Mitigation Plan included in this contract by reference shall periodically updated by the Contractor based on changes such as changes to the legal entity, ownership, ownership relationships, the overall structure of the organization, Contractor management, subcontractor arrangements, or Contractor modification of the work scope.

(End of Clause)

H.24 SECURITY CLASSIFICATION REQUIREMENTS

- (a) Selected work performed under this contract requires that individuals performing components of the work possess a U.S. Government SECRET clearance. The work requiring a SECRET clearance includes:
- Application Development Management (mainframe and distributed)
 - Application Development Team Leads (PSR, Reporting)
 - Security Administration
 - Omni Plus Administration
 - Omni Script Developer(s)
 - Mainframe Scheduling Management
 - Network Management
 - Application Testing (PSR, Reporting)
 - Application Requirements
- (b) This work is currently performed by 8-14 individuals. The Phase-In Plan shall address how the Offeror will meet the clearance requirements specified in Section H.24 Security Classification Requirements by Day One of the basic Period of Performance.

(End of Clause)

H.25 SERVICE OF PROTEST

- (a) Protests, as defined in section 33.101 of the Federal Acquisition Regulation, that are filed directly with an agency, and copies of any protests that are filed with the General Accounting Office (GAO), shall be provided to the Contracting Officer, Marisol Vargas-Busch, 77K St NE, Suite 1000, Washington, DC 20002
- (b) The copy of any protest filed with the GAO shall be received in the office designated above within one day of Filing the protest.
- (c) A signed receipt shall be obtained from the Contracting Officer at the time of delivery.

(End of Clause)

H.26 ERRORS AND OMISSIONS INSURANCE REQUIREMENT

- (a) The Contractor represents and warrants that it has and will maintain insurance covering all operations under this Agreement, including professional errors and omissions insurance in an amount not less than \$10 million per occurrence. All insurers shall be properly licensed in their domicile and rated A-VII or better by A.M. Best or a comparable rating service and policies shall not contain non-standard exclusions.
- (b) The Contractor shall keep its Errors and Omissions Insurance in full force and effect throughout the life of the contract. The FRTIB shall be named as an additional insured on the errors and omissions insurance policy, and it shall be entitled to prompt notice of any changes to coverage. In no event shall it be provided notice of any proposed changes to the errors and omissions insurance less than five business days prior to such change taking effect

(End of Clause)

H.27 DISPUTE RESOLUTION

- (a) During performance of the TESS contract, the parties agree to negotiate in good faith to resolve any disagreements.
- (b) All disputes will be initially addressed in the Program Management and Governance Structure in accordance with Paragraph 2.6 of the statement of work and elevated to the TESS Program Executive Committee (TPEC).

- (c) If agreement cannot be reached through the TPEC, the Contractor may request either a corrective action or an equitable adjustment which must be submitted to the Contracting Officer within 90 calendar days of the date on which the dispute initially arose.
- (d) If the Contractor's request for corrective action or equitable adjustment is denied by the Contracting Officer, and the Contractor wishes to further pursue its claim, within 90 calendar days of denial by the Contracting Officer, the Contractor must submit its claim to a mutually agreed upon arbitrator for resolution by binding arbitration. Otherwise, the Contracting Officer's decision regarding the claim is binding.

(End of Clause)

H.28 SERVICE LEVEL MANAGEMENT TRANSITION

- (a) In order to support key operational objectives of the Agency, a Service Level Management (SLM) Transition Plan is a critical element of the TESS Contract. In order to develop and execute the SLM Plan, a Service Level Management (SLM) Transition Phase will be conducted beginning immediately after commencement of the contract to establish mutually agreeable service levels and critical service levels that will be reviewed and updated in the SLM Plan on an annual basis. The Offeror shall initiate and organize a meeting within two weeks after commencement of the contract to begin the SLM Transition Phase. Changes to service levels will be executed through the change management process.
- (b) The key Objectives of the SLM Transition Phase are:
- To review the service levels as provided in the TESS RFP SOW Attachment in order to identify service levels that are manageable, attainable, and realistic
 - To identify the "critical" service levels that are applicable for service credits as a result of not achieving service level targets
 - To measure service levels in order to establish a baseline performance level for each service level in order to set the service level targets
 - To provide monthly service level performance reports beginning after the Phase-In period (First 60 days) that will be reviewed in monthly service level meetings for the duration of the contract
 - To establish the Service Level Management Plan.
- (c) The Offeror will be responsible for implementing the Service Level Management (SLM) Plan. Should the Offeror and FRTIB be unable to agree

to a SLM Plan at the end of the SLM Transition Phase, FRTIB at its sole discretion will be entitled to engage an independent third party to develop the Service Level Management Plan, to which the Offeror will be responsible for implementing. If the Offeror does not implement the SLM Plan to the satisfaction of FRTIB, FRTIB may consider it a breach of the Offeror's contractual responsibilities.

(End of Clause)

H.29 INFORMATION SYSTEM(S) ARCHITECTURE

The Contractor shall ensure that all of their Information Systems comport to the following requirements:

(a) Segregation Of Contractor Information System(s)

The Contractor shall establish and maintain dedicated, segregated information system(s) (e.g., servers, desktops, and data networks) for the purposes of supporting this contract. The Contractor shall ensure that the design of any logical segregation techniques used to achieve this requirement is included within the information system(s) security plan.

(b) External Interconnection(s)

The Contractor shall only interconnect their information system(s) with FRTIB's information systems. The Contractor shall not establish any physical or logical interconnections between Contractor-owned information systems supporting this contract and third-party information systems (including the Internet) without FRTIB's approval. The Contractor shall ensure that approved external interconnections are designed and monitored in a manner that does not permit the third-party information system to be able to access FRTIB's information systems.

(c) Remote Access

FRTIB will provide remote access to FRTIB's and Contractor-owned information system(s) for Contractor's employees through FRTIB's established Remote Access points. Contractor shall ensure that all Contractor-owned end-user devices (desktops, laptops, etc.) support FRTIB's Remote Access points. Contractor shall be responsible for ensuring that Contractor-owned end-user devices are properly configured.

FRTIB may require an assessment (compliance with standard configuration settings, application of security updates, etc.) of end-user devices at the time of a remote access connection and may limit or deny access to non-compliant devices.

(d) Administration And Security

The Contractor shall integrate, under FRTIB's control, administrative and security components (e.g. Windows Domains) with FRTIB's information systems.

(e) Compatibility And Supportability

The Contractor shall ensure that Contractor-owned information system(s) are compatible and remain compatible with FRTIB's information systems. The Contractor shall ensure that Contractor-owned information systems remain within manufacturer support at all times.

(End of Clause)

H.30 FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE (DEC 2012)**(a) Definitions.**

- (1) "FOCI package," as used in this clause, means a complete set of Foreign Ownership, Control, or Influence (FOCI) documents to include a Standard Form 328, Certificate Pertaining to Foreign Interests (SF 328), an Organizational Entity Structure (OES) form when there is a parent level entity, and a Key Management Personnel List (KMPL).
 - (2) "Domestic operational parent," as used in this clause, means a U.S. entity which exercises operational control over its subsidiaries and affiliates. It does not include a holding company or a passive investment company.
- (b) Notwithstanding the provisions of Chapter 2 Section 3 of the National Industrial Security Program Operating Manual (NISPOM), February 2006, the Sponsor intends to secure services or equipment from firms which are not under foreign ownership, control, or influence or where any FOCI may, in the opinion of the Sponsor, adversely impact on security requirements. Notwithstanding the limitation on contracting with an Offeror under FOCI, the Sponsor reserves the right to contract with such Offerors under appropriate arrangements, when it determines that such contracts will be in the best interest of the Sponsor.
- (c) Accordingly, all Offerors responding to this RFP or initiating performance of a contract are required to submit or validate a FOCI package for the Offeror or Contractor and the Offeror's or Contractor's highest level domestic operational parent, if applicable.

- (1) An Offeror or Contractor shall submit its FOCI package at the company or

subsidiary level, not at the branch or division level. The OES shall include the complete ownership chain from the highest parent, domestic or foreign, down to any subsidiaries or affiliates the contracting entity may own.

- (2) A separate FOCI submittal consisting of an SF 328 and a KMPL is also required at the highest level domestic operational parent entity level of the Offeror or Contractor when such a relationship exists.
 - (3) In accordance with the Certification of Foreign ownership, Control, or Influence provision Incorporated in Section K, the Offeror can satisfy the requirements of this clause by certifying that the Sponsor's FOCI records are current and correct. New or updated FOCI packages can be submitted in either one of the two methods as described in paragraph (e) below.
 - (4) All affirmative answers contained In a SF 328 must explain the identity, nature, degree, and impact on its organization or activities. The Sponsor reserves the right to request additional information.
 - (5) The KMPL must identify the Company Security Officer (CSO) and the required senior management by name, position, social security number, date/place of birth, citizenship status, ownership interest in the company, security clearances and any supplemental information which may be requested.
- (d) The Contractor shall report any changes in FOCI status and KMPL information during the period of performance of this contract to the Contracting Officer and submit FOCI packages in accordance with paragraph (e). An updated SF 328 is required of the Contractor or any of its subcontractors whenever there is a change in a response to any of the 10 questions on the SF 328. An updated KMPL is required whenever there is a key management personnel change. Failure to provide timely notice may result in termination of Sponsor accredited locations.
- (e) The Contractor shall provide FOCI packages and/or updates to the FOCI Program via Hard Copy Submittal or in accordance with the alternate e-FCL/e-FOCI Method.
- (1) Hard Copy Submittal to FOCI Program:
Office of Contracts
Attn: Jordan S. Blake PO Box 40843
Arlington, VA 22204
 - (2) Duplicate Hard Copy Submittal and notification of e-FOCI submittal to the Contracting Officer:
Marisol Vargas-Busch
Contracting Officer
77 K St NE, Suite 1000

Washington, DC 20002

- (f) The FOCI program is centrally managed by a staff responsible for determining if the Offeror or Contractor is FOCI eligible or FOCI mitigated. The Contractor shall promptly disclose to the Contracting Officer and the FOCI program any information pertaining to any interest or suspicious activity of a FOCI nature at the Contractor or its subcontractors.
- (g) If a Contractor is operating under FOCI mitigation through the Defense Security Services (DSS), the Contractor shall provide a copy of its agreement with DSS to the FOCI address in paragraph (e), as well as any updates to its agreement throughout the duration of any Sponsor accredited locations. The Contractor shall operate in strict accordance with Its DSS FOCI mitigation.
- (h) The Offeror or Contractor is required to request, collect, and forward to the Sponsor complete FOCI packages from all potential subcontractors undertaking classified work under the Offeror's direction and control with its proposal and through the entire period of performance of the contract. Offerors are responsible for the thoroughness and completeness of each subcontractor's FOCI package. The alternate e-FCL/e-FOCI method is available for subcontractors. When selecting this method, the "Alternate e-FCL/e-FOCI Method of FOCI Submittal Form shall be attached to the "SubContractor Notification Form" in lieu of the FOCI package.

(End of Clause)

H.31 DIRECTIVE AND POLICY COMPLIANCE

The Contractor shall comply with all applicable directives and policies set forth in Section J Attachments.

(End of Clause)

H.32 ACCESS TO SENSITIVE INFORMATION

- (a) As used in this clause, "sensitive information" refers to FRTIB or TSP data and information that qualifies for an exception to the Freedom of Information Act, which is not currently in the public domain, and which may embody trade secrets or commercial or financial information, and which may be sensitive or privileged.
- (b) To perform work under the TESS contract, the Contractor shall:
 - (1) Use any sensitive information coming into its possession only for the purposes of performing the services specified in this contract, and not to improve its own competitive position in any procurement.
 - (2) Safeguard sensitive information coming into its possession from

- unauthorized use and disclosure.
- (3) Allow access to sensitive information only to those employees that need it to perform services under this contract.
 - (4) Preclude access and disclosure of sensitive information to persons and entities outside of the Contractor's organization.
 - (5) Train employees who may require access to sensitive information about their obligations to utilize it only to perform the services specified in this contract and to safeguard it from unauthorized use and disclosure.
 - (6) Obtain a written affirmation from each employee that he/she has received and will comply with training on the authorized uses and mandatory protections of sensitive information needed in performing this contract.
 - (7) Administer a monitoring process to ensure that employees comply with all reasonable security procedures, report any breaches to the Contracting Officer, and implement any necessary corrective actions.
- (c) The Contractor will comply with all procedures and obligations specified in its Organizational Conflicts of Interest Avoidance Plan, which this contract incorporates as a compliance document by reference.
- (d) The nature of the work on this contract may subject the Contractor and its employees to a variety of laws and regulations relating to ethics, conflicts of interest, corruption, and other criminal or civil matters relating to the award and administration of government contracts. Recognizing that this contract establishes a high standard of accountability and trust, the Agency will carefully review the Contractor's performance in relation to the mandates and restrictions found in these laws and regulations. Unauthorized uses or disclosures of sensitive information may result in termination of this contract for default, or in debarment of the Contractor for serious misconduct affecting present responsibility as a government contractor.

(End of Clause)

H.33 Contract Type

The Agency reserves the right to negotiate a change in contract type from Cost Plus Fixed Fee (CPFF) to Cost Plus- Incentive Fee (CPIF) for Core CLINs at any time during the performance of this contract. The contractor's proposed costs shall not be adjusted upward as a result of this action.

(End of Clause)

(End of Section H)