

Department of Justice (DOJ)
Information Technology Support Services (ITSS) 5
Request for Proposal (RFP)



DJJP-16-RFP-xxxx

Month dd, 2016

DRAFT - FOR INDUSTRY COMMENT ONLY

TABLE OF CONTENTS

PART I – THE SCHEDULE.....	4
SECTION A – SOLICITATION / CONTRACT FORM (SF 33 - cont'd).....	4
A.1 Contract Type	4
A.2 Business Size Classification.....	4
SECTION B – SUPPLIES OR SERVICES AND PRICES OR COSTS.....	5
B.1 General	5
B.2 Minimum and Maximum Amounts	6
B.3 Pricing Tables	6
B.5 Supplies and Services Related Provisions.....	11
B.6 Travel Expenses	11
B.7 Other Unallowable Costs	12
The Remainder of this Page Intentionally Left BlankSECTION C –	
DESCRIPTION/SPECIFICATIONS/WORK STATEMENT	12
C.1 Introduction and Background.....	13
C.2 ITSS-5 Contract Objectives.....	13
C.3 Scope of ITSS-5 Contracts	14
C.4 Contract Management and Administration	14
C.5 Support Services.....	22
C.6 Staffing Requirements	37
C.7 Government Furnished Property and Equipment	39
SECTION D – PACKAGING AND MARKING	40
D.1 Payment of Postage and Fees	40
D.2 Preservation, Packing and Marking.....	40
SECTION E – INSPECTION AND ACCEPTANCE	41
E.1 Inspection and Acceptance.....	41
E.2 FAR Clauses Incorporated by Reference.....	41
SECTION F – DELIVERIES OR PERFORMANCE.....	42
F.1 Term of Contract	42
F.2 Delivery Schedule	42
F.3 Observance of Legal Holidays/Federal Non-Work Days.....	42
F.4 Notice to the Government of Delays.....	43
F.5 Delivery of Redacted Proposal	44
F.6 FAR Clauses Incorporated by Reference.....	44
The Remainder of This Page Intentionally Left BlankSECTION G – CONTRACT	
ADMINISTRATION DATA	44
G.1 Responsibilities for Contract Administration.....	45
G.2 Contractor Representatives.....	46
G.3 Reports.....	47
G.4 Payment	47
G.5 Pricing of Adjustments	50
G.6 Security Programs Manager (SPM)	50

The Remainder of This Page Intentionally Left Blank

SECTION H – SPECIAL CONTRACT REQUIREMENTS

REQUIREMENTS	51
H.1 Ordering.....	52
H.2 Data and Property Rights	55
H.3 Organizational Conflict of Interest.....	56
H.6 Standards of Conduct	70
H.7 Contractor Responsibility for Assigned Space and Equipment	71
H.8 Indemnification	71
H.9 Publicity.....	72
H.10 Freedom of Information Act Requests for Contractor’s Proposal	72
H.11 Subcontracts and Administrative Contracting Officer (ACO) Consent	72
H.12 Prohibition Against Soliciting and Performing Personal Services.....	73
H.13 Insurance	74
H.14 Type of Contract (APR 1984) FAR 52.216-1	74
H.15 Small Business Subcontracting Plan Requirements	74
H.16 Facility Access	75
H.17 Personnel Requirements (Hiring).....	76
H.18 Confidentiality of Data.....	76
H.19 Government Rights in Data and Computer Software.....	77
H.20 Proprietary Rights.....	77
H.21 Section 508 Compliance.....	77
H.22 Electronic Subcontracting Reporting System (eSRS) – Interim Procedures	77
H.23 Clauses Incorporated by Reference.....	78
H.24 Off-Ramp.....	78
H.25 On-Ramp	78
H.26 Open Season Procedures	79
H.28 Continuing Contract Performance during a Pandemic Influenza or other National Emergency.....	79
NOTE: Sections I, J, K, L, and M are not included for Industry Comment.....	81

PART I – THE SCHEDULE

SECTION A – SOLICITATION / CONTRACT FORM (SF 33 - cont'd)

A.1 Contract Type

- (a) ITSS-5 is a Multiple Award, Indefinite-Delivery, Indefinite-Quantity (IDIQ) Program. Each IDIQ contract has a schedule of fully burdened and fixed unit price Labor Hour rates and Other Direct Cost (ODC) line item categories, with reasonable handling charge factors. ITSS-5 includes two IDIQ award tracks: one for contracts awarded to Small Business firms and the other for contracts awarded on an unrestricted basis. At the time of award, each ITSS-5 contract will obligate a guaranteed minimum amount of U.S. dollars (amount to be determined), as set forth in Section B.2, which will satisfy the Government's minimum obligation for the life of the contract.
- (b) Task orders shall be awarded on a firm fixed price (FFP), labor hour (LH), or time and materials (T&M) basis as appropriate. ITSS-5 contractors shall compete independently for task awards pursuant to the provisions set forth in Section H herein. As a general policy, all task order requirements will be subject to a small business set-aside determination made by the Administrative Contracting Officer (ACO). The Department of Justice (DOJ or Department) will solicit individual task orders on a small business set-aside basis if the ACO determines there is a reasonable expectation of obtaining competitive offers from at least two small business concerns.

A.2 Business Size Classification

(a) NAICS Code and Size Standard. The NAICS code assigned to this procurement is 541512 - Computer Systems Design Services. The corresponding small business size standard for the NAICS code assigned is \$27.5 million in average annual receipts over the past three years. This means that if a prime contract Offeror averaged receipts is over this amount, it must certify itself as a "Large" business under this procurement in Section K.7, and submit a Small Business Subcontracting Plan (See Attachment 5), even if it is otherwise considered a "small business" under other federal contracts, or under other NAICS codes.

SECTION B – SUPPLIES OR SERVICES AND PRICES OR COSTS

B.1 General

(a) The Contractor shall provide, in accordance with the requirements specified herein, all labor, management, supervision, and other resources necessary to furnish Information Technology Support Services 5 (ITSS-5) support services to the Department of Justice (DOJ). All ITSS-5 requirements shall be fulfilled on an Indefinite Delivery/ Indefinite Quantity (IDIQ) task order basis. This contract does not qualify as a Government Wide Agency Contract (GWAC). Only DOJ Bureaus and Components are authorized to use the ITSS-5 multiple award contract vehicle.

(b) The principal purpose of this contract is to provide non-personal, labor hour services which cover a wide range of Information Technology (IT) related tasks and processes as described in Section C herein. DOJ considers the *principal purpose* of this contract to be for the furnishing of hourly based services through the use of employees exempted from the Service Contract Act (SCA). Therefore, ALL labor categories and hours published herein are considered exempt from SCA, unless otherwise explained by the offeror in its proposal and accepted by the Government at the time of award. This contract also allows for the acquisition of IT hardware, IT software, IT communications technology, or other equipment & supplies ONLY if a total system solution is solicited and such equipment is integral to the specific task effort. In this instance, only the initial purchase and installation of equipment is authorized. Subsequent upgrades in equipment and/or software, and maintenance to same shall be procured by the DOJ separate and apart from ITSS-5.

(c) During contract performance DOJ intends to continuously monitor the relative value of the labor hour based IT support services compared to the combined value of the IT hardware, IT software, IT communications technology, and other equipment acquired and reserves the right to limit the acquisition of these items going forward.

(d) The ITSS-5 projected contract term for placing orders will cover a ten year period as shown below:

Period	Beginning	End
Base Period	Date of Contract Award	Five years thereafter
Option Period 1 (OY1)	From award of 1 st Option	Five years thereafter

(e) The actual start date for the Base Period and the end date for Option Period 1 (OY1) will be inserted at contract award. See Section F.1 for complete contract term and option information.

(f) The contract ordering period may be extended beyond Option Period 1 (OY1) for a period not to exceed six months under the Option to Extend Services provision, Section F.1.2 of this contract. The fixed unit prices for this extended period, if exercised by the Government,

shall be those as set forth for OY1 in Attachment 1 herein. The Contractor has considered this fact in making its pricing proposal for OY1.

(g) The performance of all work under this contract shall be initiated by the issuance of task orders, also known as “Work Plan Requests” (WPRs) as discussed in C.4.2 and H.1, by the Contracting Officer. Task orders may be issued at any time during the base and/or option period.

(h) Indefinite-Delivery, Indefinite-Quantity (IDIQ), Blanket Purchase Agreements (BPAs), and Letter Contracts are not permissible task order types under the ITSS-5 Program. Orders for which IT services are not the principal purpose, for example, orders for which supplies, equipment and/or software/hardware services are the principal purpose are not permissible task order types.

(i) Performance of task work may extend beyond the contract expiration date(s) specified above for a period not to exceed one hundred and eighty three (183) calendar days (i.e. six months) from the expiration date of the contract. Orders may be placed up to and including the last day of the contract. See Section H.1.1 for the complete provision.

B.2 Minimum and Maximum Amounts

(a) The Department will order a minimum amount of **\$5,000** for every contract awarded. The Department will order services within the contract period of performance (to include option years if applicable) sufficient to satisfy the minimum guaranteed amount for each ITSS-5 contract awarded. Should the Government decide not to exercise the option period and the guaranteed minimum amount has not been satisfied, the minimum amount will be ordered in the last year of contract performance. If the guaranteed minimum amount has been paid to the contractor, the exercise of the option does not re-establish the contract minimum. The specific Contract Line Item Numbers (CLINs) and quantities will be identified in one or more task order(s) issued under this contract.

(b) There are no specific maximum quantities/amounts for each individual CLIN, task order, contract period, or contract. The Department may order items in any quantity up to the maximum aggregate amount limit for all task orders. The maximum aggregate amount of all task orders issued under all the ITSS-5 contracts shall not exceed **\$1,400,000,000** for the entire term of the contracts, including the option period which may be exercised.

B.3 Pricing Tables

See Attachment 1 for the Microsoft Excel 2010 .xls template for all Section B Tables.

(1) The following Definitions apply to the B-1 Unit Price Tables (CLINs X001 - X049):

- (a) Government Site and Rates (Table B-1.1):
 - (i) Work/services performed on a continuous regular basis at a Government controlled site to include basic office space, office equipment, and office supplies provided by the Government. This

- may be Government owned space or commercial space leased by the Government. The unit prices set forth shall contain all costs associated with providing and delivering the support services at a Government controlled facility(ies).
- (ii) The unit prices shall include all expenses, including, but not limited to salaries/wages, fringe benefits, overhead on direct labor, G&A, and a reasonable profit. The unit prices shall exclude the cost of the contractor's or subcontractor's facility, office furnishings, office supplies and office equipment to include desktop personal computers, since these are primarily government furnished items. The unit prices shall include factors for management and administration duties as described in Section C.4 and the contract level reports described in C.4.5 and G.3. However, if the task order specifically requires a logistical service or a detailed status report for that task, the time expended for those direct services will be billable at the appropriate hourly rates.
 - (iii) A single set of rates is provided regardless of whether the services are provided by the prime or by a teaming partner or subcontractor. The contractor shall indicate in the column provided if it is the principal provider of each CLIN, or if a teaming partner or subcontractor is the principal provider.
- (b) Contractor Site and Rates (Table B-1.2):
- (i) Work/services performed on or at the Contractor's or teaming partner's or subcontractor's site. The unit prices set forth shall contain all costs associated with providing support services at the Contractor's or subcontractor(s) facility(ies) and delivering the output of those efforts to the Government.
 - (ii) The unit prices shall include all expenses, including, but not limited to salaries/wages, fringe benefits, overhead on direct labor, G&A, a reasonable profit, equipment usage, and computer resources (defined as "in-house" computer resources which are utilized by the Contractor at its site in the performance of work comparable to that required under this contract, including personal computers for Contractor staff and all Section C.4.1 requirements). The unit prices shall include factors for management and administration duties as described in Section C.4 and the contract level reports described in C.4.5 and G.3. However, if the task order specifically requires a logistical service or a detailed status report for that task, the time expended for those direct services will be billable at the appropriate hourly rates.
 - (iii) A single set of rates is provided regardless of whether the services are provided by the prime or by a teaming partner or subcontractor. The contractor shall indicate in the column provided if it is the principal provider of each CLIN, or if a teaming partner or subcontractor is the principal provider.

- (c) The greater Washington, DC (WDC) area is defined as:
- (i) the U.S. Census Bureau's Combined Statistical Area (CBSA) No. 548 covering Washington, DC; Baltimore, MD; Northern Virginia; and the two West Virginia panhandle counties. All rates in Table B-1 shall be based on performing the services in the CBSA No. 548 area. The DOJ's experience has been that about 99% of the work under the ITSS program has been performed in the greater WDC area, and most of that percentage is actually in WDC or the immediate surrounding counties. Non-personal support services may be provided anywhere in the United States and its territorial possessions, and occasionally in foreign countries when specific authorization has been provided by the Government.
 - (ii) If a specific task requirement calls for work to be performed outside the greater WDC area as defined above, then the contractor(s) competing for that task order may propose an appropriate adjustment factor for areas that have a substantially higher (or lower) cost of living index than the WDC area. Under this scenario, the Table B-1 Tables are taken as a baseline of 1.000, and a task offeror would propose a factor of 1.xxx to all the labor categories and rates proposed for that task. For example, for an area which has a cost of living index approximately 5.5% higher than the WDC area, taking into effect the relative costs of housing and office space, the proposed rate adjustment factor would be 1.055. However, the burden is on the offering task Contractor to justify and document any proposed adjustment factors to the B-1 rates in making a specific task proposal when the work is outside the greater WDC area. Competitive forces and management challenge may also play a role in determining what adjustment factors are proposed by the ITSS-5 contractor(s).
- (2) Overtime Rates Not Solicited: Overtime premium rates are not solicited or authorized under the ITSS-5 contracts, except for extremely unusual conditions to be specified on a rare individual task order. Therefore, all of the hourly rates for all Table B-1 CLINs shall reflect the conditions below:
- (a) One Rate Set: The singular billable rate for hourly personnel acquired via task order, or the singular billable hourly rate for salaried personnel acquired via task order. One set of rates is solicited, regardless of when these services may actually end up occurring. The vast majority of the work occurs Monday - Friday during standard workday hours, excluding Federal Holidays. This is also known as a "Normal" work schedule rate set in the B-1 Tables.
 - (b) Uncompensated Overtime. DOJ does not expect that the contract rates include decrements for uncompensated overtime conditions, for example, when evening time is worked by salaried professional employees on proposal preparation efforts. FAR Clause 52.237-10 Identification of Uncompensated Overtime (Oct 1997), applies to this solicitation/contract.

(3) **Table B-2, Other Direct Costs and Handling Charge Factors.** This Table delineates five (5) CLIN groups which are considered allowable other direct costs (ODC) and under task orders issued on a time-and-materials basis, or as may be used to price a task order issued on a firm fixed-price basis. The table provides cells for the contractor's fixed ODC rates. [Note that the requirements of Section C.4.1 are not separately billable and will not be considered allowable ODCs under this contract. Costs for such items shall be built into the Table B-1 unit prices.]

- (A) **Government Estimated Other Direct Costs (ODCs).** For each CLIN group of ODCs, the DOJ has estimated an annual amount of dollars for evaluation purposes only, which are known as "the raw ODC given amounts". The actual amount expended may range from zero dollars (\$) to a dollar amount higher than the raw ODC given amounts. The Government is under no obligation to purchase any ODCs under this contract. Also, DOJ has determined it is appropriate and prudent to place ceilings on the Handling Charge Factors (HCFs) as set forth below. For any contract awarded whereby the HCF is less than the ceilings indicated below, the lower HCF will become the ceiling during contract performance.

There are five CLIN groups of ODCs which are listed in Table B-2 and as follows:

ODC CLIN Group

- (a) Expert Consultants (CLIN X049) HCF is limited to a ceiling of 0.000.
- (b) IT Hardware and Communications Technology (CLIN X050) HCF is limited to a ceiling of 0.050.
- (c) IT Software (CLIN X051) HCF is limited to a ceiling of 0.050.
- (d) Other Equipment and Supplies (CLIN X052) HCF is limited to a ceiling of 0.050.
- (e) Local and Non-local Travel Expenses IAW the Federal Travel Regulations (CLIN X053) HCF is limited to a ceiling of 0.099.

Note 1: Expert Consultants are professionals with special skills, training, education, and/or abilities that the market prices at various amounts depending on the disciplines required, availability, and other factors. Under Attachment 1, the Expert Consultants (all four levels) are shown as CLIN X043. However, Expert Consultants are not pre-fixed priced in Table B-1 of this solicitation/contract.

- (B) **Utilization of Expert Consultants, CLIN X049.** The use of the Expert Consultant labor category will be authorized and limited to very specialized requirements under specific task orders. The Work Plan Requests issued under C.4.2 will state whether or not the proposing of Expert Consultants is authorized for the task order proposal.
- (C) **Handling Charge Factors.** Each ODC CLIN group specified above shall have a corresponding Handling Charge Factor (HCF) which shall offset administrative handling costs associated with procuring and managing the ODC. Full G&A shall not be added. After delivery and acceptance of the ODC, the actual "reasonable, allowable, and allocable" direct cost of the item will be reimbursed plus the handling charge amount as calculated by multiplying the ODC amount by the applicable HCF. The specific elements of cost under each Table B-2 ODC CLIN group are only allowable to the extent that they

are not included in the fixed unit prices of Table B-1 and have been authorized by the COTR. The billable amount shall be limited to the actual reasonable, allowable, and allocable cost of the item plus the amount resulting from the application of the appropriate HCF identified in Table B-2 (e.g., if the actual cost of an item is \$100.00, and the HCF for that ODC category is 0.045, the total billable amount is \$104.50). For subcontracted items/services, the HCF shall only be applied one time. For example, a subcontractor might be required to travel. It is not permissible for the subcontractor to apply a markup to the travel costs in billing the prime contractor, and then for the prime contractor to apply another markup when billing the Government. The HCF may only be applied once, and must be applied to the documented actual direct cost of the item.

(4) Table B-3, Extended CLINs and Total Estimated Price Tables (4 each)

ALL THE B-3 TABLES ARE PASSWORD PROTECTED SHEETS.

Unit Price Extensions. Tables B-3.1 and B-3.2 are the extended price tables that correspond with Tables B-1.1 and B-1.2. The B-3 tables do not require Offeror/Contractor completion of any kind and are not to be altered by the Contractor in any way. The row and cell numbers in the B-3.1 and B-3.2 tables line up perfectly with the Tables B-1.1 and B-1.2.

Table B-3.3. This table is the government provided raw estimated ODCs times HCFs shown in Table B-2 to determine the handling charge amount, plus the raw ODC amount. Table B-3.3 does not require Offeror/Contractor completion of any kind and is not to be altered by the Contractor in any way. The row and cell numbers in B-3.3 line up perfectly with the B-2 table.

B.4 Pricing Adjustments - Option Period One

(a) The actual contract ceiling rates and ceiling multipliers for Option Period One (1) will be determined by escalating the proposed Year Five (5) ceiling rates and ceiling multipliers utilizing the latest methodology and basis for the Bureau of Labor Statistics' (BLS) Employment Cost Index (ECI).

(b) The contract adjustment will be calculated three months prior to Option Period One using the latest ECI information available at that time and implemented at the beginning of year six (Option Period One – if exercised). The Government intends to use the average of the five previous full years of ECI data to make a one-time contract escalation. This escalation will be applied one time to years six through ten ceiling rates and ceiling multipliers – to remain fixed thereafter. The calculated escalation rate will be applied consecutively for years six through ten. This means that the escalation rate will have compounding effect for years six through ten. It will be applied one time for the option period. Each year in the option period will have separate pricing as a result.

(c) For contractors that proposed to apply a reduced escalation rate of 1% to 100% from the amount that will be calculated at the beginning of Option Period One, this reduced escalation rate will be reflected in the pricing adjustment.

(d) **Adjustments to Task Order Hourly Rates.** The Government does not intend to perform redeterminations or apply escalated rates retroactively. The escalation will not apply to task orders already awarded (in place) unless they specifically definitize its inclusion. Task order hourly rates may be adjusted, if specified in the task Statement of Work, for each of the task order option period years by applying no more than the same adjustment factor to the task order rates as was applied to the contract hourly rates. If an order does not specifically provide for such an adjustment, no such adjustment is permitted.

B.5 Supplies and Services Related Provisions

(a) Supplies purchased and services procured are subject to FAR Clause 52.229-3 Federal, State, and Local Taxes (APR 2003). The stated fixed prices for the Table B-1 and B-3 Labor Hour services herein include all taxes.

(b) For leased equipment under this IDIQ contract, if ordered as an ODC, FAR Clause 52.229-1 State and Local Taxes (APR 1984) shall apply. The Department will reimburse the Contractor for State and local taxes that must be paid by the Contractor on allowable leased ODCs, when appropriate supporting documentation is provided by the Contractor.

(c) If in the Government's best interest, the Contracting Officer may issue a letter(s) to the Contractor authorizing the Contractor to utilize Federal sources of supply (e.g., General Services Administration FSS schedules) for supplies and services procured on behalf of the Government under this contract.

(d) Price Adjustments Under the Service Contract Act. The Government-provided labor categories are not subject to the Service Contract Act (SCA) of 1965 as amended (See Section I, Clause 52.222-41); however, Contractor proposed labor categories at the task order level may be subject to the SCA. In the case that the Contractor proposes use of labor categories which are subject to the SCA, the Government will not be liable to the Contractor for any additional/increased sums/costs for which the Contractor may become liable to its employees as a result of a failure by the Contractor to properly correlate, conform or exempt its employees to the labor classifications stated in the Department of Labor (DOL) Wage Rate Determination. Final determinations as to the proper conformance or exemption of Contractor employees under the SCA will be the responsibility of the Contractor.

B.6 Travel Expenses

(a) Local Travel Expenses. As a general rule, local travel expenses shall not be reimbursed under this contract. Examples of local travel which will not be subject to reimbursement are: 1) travel to and from normal job site (i.e. commuting costs); and 2) supervisory personnel traveling to a Government site or alternative facility to oversee operations. Personnel assigned to a temporary Government site or alternative facility will consider such facility his/her normal job site. However, there are circumstances under which local travel reimbursement is allowable, such as when personnel are requested or required to attend a meeting or seminar at a local site which is not their normal job site, the local transportation expenses (e.g. metro, cab, parking, etc.) can be reimbursed. The COR specified

in Section G of this contract shall make such determinations and authorizations as appropriate.

(b) Nonlocal Travel Expenses. All nonlocal travel shall be approved in advance by the COR. Reimbursement for actual (approved) travel costs incurred during the performance of support services shall be in accordance with Part 31 of the Federal Acquisition Regulations and the Federal Travel Regulations (FTR). Travel requirements under this contract shall be met using the most economical form of transportation available. If economy class transportation is not available, the Contractor must submit (to the COR) a request for advance approval to utilize higher class travel. All travel shall be scheduled sufficiently in advance to be able to take advantage of offered discount rates. The Federal Travel Regulations and per diem rates can be accessed at: www.gsa.gov and type "FTR" in their search box.

B.7 Other Unallowable Costs

(a) Hours expended by Contractor personnel working on task order proposals are not allowable as items of direct cost and not reimbursable under this contract. Time and travel expenses to attend pre-proposal conferences for task orders are not cost reimbursable items under this contract.

The Remainder of this Page Intentionally Left Blank

SECTION C – DESCRIPTION/SPECIFICATIONS/WORK STATEMENT

Preamble: This contract and the Statement of Work (SOW) which follows allow for but do not require “performance based” service contracting. The DOJ and the Contractor encourage the DOJ components that utilize this contract to plan for and write their individual task requirements such that the Government’s overall performance based service contracting objectives are met to the maximum practicable extent.

C.1 Introduction and Background

(a) Most Department of Justice (DOJ) organizations have their own small staff of computer specialists, systems analysts, and programmers to provide information technology (IT) support services. Nevertheless, they do not maintain a sufficient staff of personnel to meet the anticipated demand for systems development and other IT support services. Nor do they maintain technical expertise in the multiplicity of equipment, operating systems, languages and applications currently in use, planned or potentially applicable within the Department.

(b) When DOJ organizations cannot fulfill their requirements using in-house staff, they often need contractor support quickly. Realizing this need, the Department decided to establish a set of contracts to provide software development and other IT-related services to Department components. Under the ITSS program the current set of nineteen contracts was awarded in March 2011 and includes a base year and six option years.

(c) Since its inception, the Department has required that the contractors under the ITSS program compete for the work at the task order level. Competition at the task order level has proven cost-effective, and has yielded significant savings. It has enabled the Government to obtain high-quality technical expertise at a reasonable cost.

(d) The ITSS contracts are available for use on a voluntary basis.

(e) Fee-for-Service. This IDIQ Multiple Award Contract vehicle may be utilized by any DOJ component (e.g. Office, Bureau, or Division) on a fee-for-service basis. The DOJ Office of the Chief Information Officer (OCIO) will coordinate with the COR specified in Section G herein, to create the specific fee-for-service schedule for the ITSS-5 program and establish Intra-agency Agreements as necessary to transfer and/or reimburse funds to DOJ to compete, award, and oversee the work plan requests and resulting task orders. The fee-for-service schedule established at the onset of this contract may change from time-to-time as determined by the Office of the CIO, but not more than once per fiscal year. The unit prices contained in this contract do not include any kind of industrial funding fee or similar charging factor.

C.2 ITSS-5 Contract Objectives

(a) The ITSS-5 contracts may be used to fulfill a wide range of requirements in any of the Systems Development Life Cycle (SDLC) areas described in Section C.5 herein. While the variety and scope of services (See C.3 below) that will be required is known, the specific tasks to be ordered over the coming years, and their distribution across the SDLC, are not clear.

Examples of task orders executed under ITSS-4 are provided as Attachment 8 to this RFP. The continuing emergence and rapid adoption of new technologies by Government agencies strongly suggest that the very nature of IT support services tasks will not necessarily resemble that of prior years. Large-scale systems integration acquisitions, new applications within DOJ component organizations, and the integration of and modifications to current systems will have significant impacts on future development efforts in DOJ agencies.

(b) The Department anticipates that the ITSS contracts will be used to provide IT services that:

- (1) Go beyond sustaining and expanding use of current hardware, operating systems and software.
- (2) Increase business effectiveness and automation through the effective use and adoption of systems by leveraging new technologies and applications, best practices, and software.
- (3) Create new applications and introduce new technologies as they emerge.
- (4) Give expert assistance in configuring and managing computer hardware, software and networks, in training users, and in improving systems and network security.
- (5) Facilitate business change and flexibility by architecting, designing, and developing solutions that enable the rapid realization of new or changed requirements.
- (6) Protect the business by ensuring that systems, applications, and practices are secure.
- (7) Measure and continually improve customer service and satisfaction.

C.3 Scope of ITSS-5 Contracts

(a) The ITSS-5 multiple award contracts are available for use by the entire Department of Justice on an indefinite delivery, indefinite quantity, task order basis to provide the full range of information technology support services, spanning the entire Systems Development Life-Cycle. The scope for ITSS-5 also includes the potential acquisition of hardware, software, and other equipment to support client needs as specified in B.1(b). The scope of each ITSS-5 contract will cover the full range of SDLC and functional areas for both Unrestricted and Small Business Contractors. Non-personal support services may be provided anywhere in the United States and its territorial possessions, and occasionally in foreign countries when specific authorization has been provided by the Government. Information on DOJ agencies can be found at <http://www.justice.gov/>.

C.4 Contract Management and Administration

C.4.1 General

(a) The Contractor shall provide all management, administration, staffing, planning, and scheduling for all services required by the contract and/or task order. These activities include, but are not limited to:

- (1) All activities associated with preparing proposals in response to the Department's Work Plan Requests (see Section C.4.2), submitting the proposals to the Department, and negotiating task order requirements.
- (2) All activities associated with recruiting and hiring staff, such as advertising, screening applicants, interviewing, reference checking, etc.
- (3) Maintaining "in-house" skills, teaming and/or subcontract arrangements to ensure that staff with the requisite experience, skills and knowledge are available on short notice.
- (4) Screening and processing prospective contract staff to ensure all Contractor employees used under this contract meet personnel hiring and security clearance requirements.
- (5) All activities associated with management of the Contractor's facilities that may be utilized, including obtaining space, equipment, furniture, supplies, maintenance, etc.
- (6) Utilizing electronic means to conduct business transactions under this contract to the maximum extent feasible. This will include, but is not limited to, Contractor receipt of Work Plan Requests, Contractor submission of proposals in response to such requests, Government/Contractor electronic mail exchange to support administration of active task orders, Contractor invoicing, and electronic funds transfer for payment of approved invoices.

Note: *After contract award, the Contractor and the Contracting Officer will agree on the methods and scope of electronic communications that the Contractor shall follow during the contract period.*

- (7) Ensuring facilities used for the Contractor's performance of this contract meet all physical security requirements of the contract.
- (8) Planning, scheduling and procuring airfare, lodging accommodations, and ground transportation for all approved travel by Contractor personnel. Ensuring that invoiced travel costs are itemized in accordance with the Government travel guidelines in effect at the time of travel (See Section B.5).
- (9) Planning for and making all necessary arrangements to ensure that Contractor personnel performing field work have all necessary supplies and equipment by the time they arrive at the site.
- (10) Procuring items/services on behalf of the Government. Ensuring that open

market procurements are properly documented to prove price competition was obtained, or justification for not obtaining competition. If use of GSA schedules is authorized, the Contractor shall follow the requirements of FAR Subpart 8.4 before placing the order.

- (11) Assembling billing data and billing back-up materials, including all time and materials needed for preparing any responses to Government billing rejection letters. Generating, distributing, and tracking invoices, including generating reports and responding to inquiries regarding invoice status, tracking which deliverables and/or units have been invoiced and which have not, etc.
- (12) Tracking and reporting on Government furnished materials. The Contractor is responsible for adequate care and safekeeping of all Government furnished materials, including inventorying, tracking and reporting, etc. The Contractor shall reimburse the Government for any Government furnished materials damaged, lost or stolen while in the Contractor's safekeeping.
- (13) All activities associated with managing subcontractors/team members, such as identifying and qualifying personnel, negotiating subcontracts, reviewing invoices, ensuring compliance with the security and other requirements of this Contract, etc.

The above items are not separately priced or billable under the contract or any task order.

C.4.2 Work Plan Requests

(a) Generally, all task orders will be initiated by a Work Plan Request (WPR) to be issued by the COTR. The WPR process is defined in Attachment 7 – Task Order Administration Plan.

C.4.3 Contractor's ITSS-5 Program Management Responsibilities

(a) The Contractor shall institute and maintain a program management structure to respond to and negotiate WPRs. The Contractor shall also maintain access to resources that can be called upon to fulfill task order requirements under the contract. The Department will not issue a separate task order to institute or maintain these capabilities.

(b) The Contractor's ITSS-5 program management office shall be located within a reasonable radius (approximately 50 miles) of the Department of Justice headquarters at 950 Constitution Avenue, NW, Washington, D.C., including the necessary resources (i.e. management, technical and financial personnel working in that location) needed to support the ITSS-5 program. The location must be that which allows for the Contractor's staff to be able to travel to DOJ headquarters within a reasonable timeframe upon receiving an urgent call from the COTR or a higher level DOJ IT manager.

(c) For each task order issued to the Contractor, the Contractor shall maintain a management structure with overall task order control and authority for the performance of work. The Department may request a Program Management Plan as part of a WPR. At a minimum, the Contractor's management structure shall be responsible for the following throughout the life

of each task order:

- (1) Deploying and maintaining a technically proficient and professionally capable staff.
- (2) Keeping personnel turnover to a minimum and ensuring individuals are motivated to achieve excellent performance.
- (3) Ensuring problems are minimized and unavoidable problems are resolved with minimal disruption to the activities performed under the task order.
- (4) Obtaining continuous feedback on performance from appropriate Government personnel and disseminating feedback to Contractor personnel on all areas of task order performance.
- (5) Continually monitoring the quality of all products and services provided under the task order for purposes of identifying and implementing performance improvements.
- (6) Ensuring that all resources necessary to perform the task order are identified with clearly defined roles and deployed on schedule.

C.4.4 Staffing

C.4.4.1 Program Manager

(a) The Program Manager is a senior manager responsible for coordinating the management of all work performed under this contract. The Program Manager is ultimately responsible for coordinating the efforts of subcontractors, team members, vendors, etc. The Program Manager shall act as the central point of contact with the Department and shall have the full authority to act for the Contractor in the performance of the required work and services under all task orders. The Program Manager works independently or under the general direction of senior level Contractor business management on all phases of performance, including contract management, project/task order management, coordination of resource needs, coordination with corporate resources and management, and has direct accountability for the technical correctness, timeliness and quality of deliverables. The Program Manager shall have broad and deep knowledge of the IT industry, PMBOK (project management body of knowledge), business administration, and human resource management. It is strongly encouraged that the Program Manager be Project Management Professional (PMP) certified. The Program Manager shall have excellent oral and written communications skills. The Program Manager shall ensure that the Contractor has the capability of performing all the work.

(b) The Department will not issue a task order exclusively for the Program Manager's services. However, the Contractor may propose directly billable hours for the Program Manager in response to a WPR.

C.4.4.2 Key Personnel

- (a) The Department reserves the right to review the qualifications of all staff identified as

“Key Personnel” that are selected to work on any task order before assignment, including the individuals proposed (in the Contractor's proposal submitted in response to a WPR) and any replacements for these individuals, and to reject individuals who do not meet the qualifications set forth in this contract. Any exceptions to the labor category qualifications require written approval from the COTR.

(b) The Department reserves the right to require the Contractor to remove or reassign from this Contract any “Key Personnel” Contractor employee(s) who is/are deemed incompetent, careless, unsuitable or otherwise objectionable, or whose continued employment under the contract is deemed contrary to the best interests of the Government. Failure of “Key Personnel” Contractor employee(s) to comply with the standards of conduct specified in Section H.6 or on a specific task, may also be grounds for the Department or the client agency (thru the Department) to require removal or reassignment of offending Contractor employee(s).

(c) The Contractor shall remove or reassign any “Key Personnel” employee from performance of Contract tasks within five (5) working days of receiving a written notice from the Contracting Officer that the employee's performance or conduct is unsatisfactory or unacceptable. Further, the Contractor shall immediately remove any “Key Personnel” Contractor employee found to represent a real or anticipated threat to the safety of government records, government employees, or other Contractor employees. The Contractor shall reimburse the Department for the cost of any Department-provided or funded training given to “Key Personnel” Contractor employees who cease to perform Contract duties within six (6) months after receiving that training.

(d) The following positions/labor categories are considered “Key Personnel” positions for this Contract at the contract level:

1. Program Manager (Labor Category CLIN X001)
2. Individual task orders may identify additional labor categories/persons as key personnel such as Task Managers (Labor Category CLIN X002) or other technical staff personnel deemed important to the success of the task.

(e) Any individual performing work under the labor categories listed in paragraph (d) above is subject to the following:

- (1) Replacement of any Key Personnel is subject to the prior written consent of the COR.
- (2) Requests for replacement shall include a detailed resume containing a description of position duties and mandatory qualifications, as well as information about the qualifications of the individual(s) proposed. All replacement personnel must be qualified to assume the duties and responsibilities of the position, provide the same levels of effort as the replaced staff, and their salaries must be at similar levels of the personnel to be replaced, with no adjustment to the prices set forth in the task order.
- (3) Contractor proposals to move any Key Personnel off the Contract or from one task order to another shall be submitted in writing at least thirty (30) days in

advance of proposed move, and are subject to the approval of the COTR, including approval of proposed replacement.

- (4) In the event of a key personnel resignation, the Contractor shall notify the COTR in writing within five (5) days of receiving notice of resignation.

C.4.4.3 Training of Contractor Staff

(a) The Contractor shall be responsible for providing trained, experienced staff for performing the work ordered under this Contract, and for continuously monitoring, managing and controlling the work. The Contractor shall make its best efforts to retain staff members who have gained experience on this Contract, and to minimize staff turnover.

(b) The Contractor shall train its own staff so as to ensure that all personnel are able to perform their duties under each task order satisfactorily. This may require staff training in the specific technology area. The Contractor will furnish the COTR with formal documentation of the training provided to each labor category under the Contract as requested by the COTR, including testing tools for determining if individual employees have achieved competence in their labor categories. Except where specifically approved by the COTR, training of Contractor staff is not separately billable. Specialized training requested by the COTR beyond that which would normally be required to perform under the contract is billable.

(c) In addition to job-specific or professional training, the Contractor shall ensure its employees on this contract are trained on "contract-specific" issues such as DOJ ethics, standards of conduct, individual conflicts of interest, confidentiality requirements, DOJ security requirements, the function of reporting, and the importance of quality control and quality assurance. In addition, Contractor managers shall be educated regarding the terms and conditions of the contract.

C.4.4.4 Security Clearances, Contractor Screening Guidance, and Confidentiality Agreement

(a) Prior to assigning an employee to the contract, the Contractor must submit for that employee the completed forms as specified in Section H.4.

(b) The Contractor is responsible for screening ALL prospective employees for suitability and conduct for work on this Contract, prior to submittal of the H.4 security forms. Guidelines for this screening function are provided in Attachment 3.

(c) The ITSS-5 Contractor shall have available qualified staff with, at a minimum, the types of clearances specified in contract Section H.4. This is so the contractor may be in a position to quickly begin work if it is successful in capturing specific task orders.

(d) Attachment 3 also contains the standard DOJ Confidentiality Agreement for contractor and subcontractor employees to certify prior to commencing work under task order(s) awarded.

C.4.4.5 Quality Assurance and Quality Control

(a) The Contractor shall ensure that all documented guidelines and operating procedures for quality assurance/control are followed for all areas of performance. The Contractor shall develop and implement additional quality assurance/control procedures as necessary to ensure all work performed is in accordance with standards prescribed in this contract or individual task order for the duration of the contract, and the Contractor shall stress to its staff the importance of quality control and quality assurance. Quality practices that are consistent with Software Engineering Institute (SEI) Capability Maturity Models (CMM or CMMI) and ISO shall be achieved as follows:

- (1) Minimum assessment of CMMI Level 3.
- (2) Certification as ISO 9000.
- (3) Staff certification at ITIL Foundations level, or ITIL v3 Expert level for leadership.

(b) Within the specifications of the contract/task order, and the direction of the client agency, Contractor personnel shall perform all activities on their own initiative. This will require a high degree of resourcefulness and the exercise of sound judgment. Contractor personnel shall perform the contract activities independently and shall exercise professional judgment and discretion in making decisions and recommendations for the successful completion of the activities. As appropriate, the Program Manager shall make suggestions to the client agency to improve operations. The Program Manager shall obtain client agency approval prior to implementing any precedent-setting decisions.

(c) The importance to the Department of quality control cannot be overstated. The Department is committed to quality work and will not tolerate sub-standard work. Frequently, work must be performed under rigid time constraints where the same attention to detail and quality must be observed. The Contractor must build additional quality control reviews, as needed, into the operating procedures for each functional area of the contract and task order. The Contractor shall conduct internal quarterly reviews of each task order to address the following:

- (1) Ensure personnel are following all established guidelines and procedures.
- (2) Identify appropriate modifications to procedures or other corrective actions to improve efficiency or remedy deficiencies.

(d) After each review, the Contractor shall provide a written findings and recommendations report to the COTR and client agency.

C.4.5 Management Reports

(a) The Contractor shall prepare and deliver to the COTR regular reports on work activities, Contractor expenditures, accomplishments, and the status of projects. The COTR will approve the format of each report. The Contractor shall modify the format or subject content of the reports at the direction of the COTR. Additionally, the COTR may require the Contractor to submit *ad hoc* reports (oral or written) on the work, as needed.

- (1) Contractor Personnel Security Status Report. The purpose of this report is to

maintain current and accurate records of the hiring and related clearance status of all Contractor personnel who have submitted security clearance packages. To support this function, the Contractor shall conduct a quarterly review of its personnel actions and update the following information for each individual:

- a. Employee name
- b. Contract labor category (CLIN number and name)
- c. Date request letter sent to COTR
- d. Date hiring clearance package sent to DOJ
- e. Date hiring clearance granted
- f. Start and termination dates
- g. Dates building pass issued and revoked
- h. Comments

The Contractor Personnel Security Status Report shall be delivered to the COTR on a day to be specified by the COTR following the close of the reporting period.

- (2) Government Owned Property Report. The purpose of this report is to maintain current and accurate records of the property type, location, identification number, and quantity of any property furnished to the Contractor by the Government or acquired by the Contractor on behalf of the Government for use under this contract. The Contractor should note that this may include furniture, computer and other equipment, computer software, etc. To support this function, the Contractor shall conduct a semi-annual review of all Government owned property in its custody and document and update the holdings. The Government Owned Property Report shall be delivered to the COTR at the close of business on a day to be specified by the COTR following the close of the reporting period. A copy of the most recent report shall also be delivered to the Contracting Officer by each December 31. The Government Owned Property Report shall contain, at a minimum, the following information:

- a. Item type
- b. Item description
- c. Make and model
- d. Serial number
- e. DOJ inventory number
- f. Leased or purchased
- g. Month/Year invoiced, if purchased for DOJ
- h. Warranty/maintenance information
- i. Current location (building/room)
- j. Previous location or disposition
- k. Project for which originally acquired
- l. Acquisition cost (if known)
- m. Property Classification
 1. Land and Rights Therein
 2. Other Real Property
 3. Plant and Equipment
 4. Special Tooling
 5. Special Test Equipment

6. Material
 7. Furniture/Furnishings
 8. Automated Data Processing Equipment
- n. Comments

At the end of this Contract, these reports will be used in conjunction with invoice records to determine government furnished materials owed by the Contractor to the government.

- a. Task Order Progress Report. A report which includes, at a minimum, a project action items list, expenditure summary, significant problems, and completion schedules. The contract status report is due by the 10th business day of every month.

(b) The Contractor shall, at a minimum, establish and maintain appropriate tracking systems which shall enable it to prepare and submit the management reports required. Creation and maintenance of these tracking systems is not separately billable. Costs for copying reports for distribution are not separately billable.

C.5 Support Services

This section describes the functional areas and corresponding Systems Development Life Cycle (SDLC) support services that may be required under task orders to be issued under the ITSS-5 contracts.

C.5.1 Functional Areas

C.5.1.1 IT Planning and Architecture

C.5.1.1.1 IT Planning

Identification, evaluation and recommendation of solutions and opportunities, including the modification and process re-engineering of existing systems to encourage and facilitate the development of integrated systems, provide added functionality and improve productivity, while taking into account all applicable federal standards and procedures and the client organization's standards and policies. Includes support for enterprise architecture planning, migration planning, implementation governance, and technology architecture. Also includes IT Strategy and Vision Development, IT Effectiveness Analysis, and IT Cost Reduction.

C.5.1.1.2 Feasibility Study

Identifies objectives, requirements, system concepts, and candidate approaches. It researches possible solutions and analyzes commercial off-the-shelf (COTS) products available for achieving the objectives. Includes familiarity with various COTS products in the federal marketplace. May include making recommendations on the approach to be taken. The feasibility studies will be used by managers to decide whether to proceed with the task.

C.5.1.1.3 Cost-Benefit Analysis

An in-depth evaluation of a given approach as to technical feasibility and/or the benefits to be gained for a specific cost. The analysis involves identifying, developing and analyzing the costs (actual and opportunity) and benefits of a given approach in quantitative terms if feasible and in qualitative terms otherwise, and preparation of a recommendation to proceed or not to proceed. The user may require that this type of analysis occur independently or with other activities comprising a full system development effort.

C.5.1.1.4 Business Process Re-engineering

A complete analysis of the processes used to generate desired products and services with a possible revamping of the entire approach. The primary drivers should always be the customer's needs. These needs ultimately dictate the scope and the level of technology investment. The issues that need to be reconciled include time, quality, customer perspective, people empowerment, efficiency and flexibility. Technology is considered a potential enabler of the new approach. Includes support for feasibility studies, cost benefit analysis, process modeling, business event modeling, organization design, business strategy, and change management/leadership.

C.5.1.1.5 Contingency Planning - (Continuity of Operations)

Identification of various disaster scenarios and development of response options to these scenarios. May include actual response support in addition to documentation development and testing of response scenarios. Development of new Continuity of Operations Plans (COOP), validation of existing COOP premises, environmental and technical requisites and pertinent existing documentation, and planning, executing and evaluating operational tests of new and existing COOPs. This may include outlining proposed revisions for the COOP, analyzing impacts of revisions on organizational and technical issues, drafting updated COOPs for internal technical review by client organization personnel, applying revisions to the COOP based on this review and conducting a summary review of the revised COOP with the client organization. In addition, may include development of new or revising the existing COOP test plan, providing technical support and related contingency orientation of client organization personnel before execution of the test plan, providing technical assistance during the test, developing contingency test evaluation reports to include recommendations for improvements to the test plan and the COOP, and revising the test plan and/or COOP as required after client organization review of the evaluation report.

C.5.1.1.6 Enterprise Architecture (EA)

Provides a comprehensive framework used to manage and align an organization's Information Technology (IT) assets, people, operations, and projects with its operational characteristics. In other words, the enterprise architecture defines how information and technology will support the business operations and provide benefit for the business.

EA accelerates Agency business transformation and new technology enablement by providing standardization, design principles, scalability, an enterprise roadmap, and a repeatable architecture project method that is more agile and useful and will produce more authoritative information for intra- and inter-Agency planning, decision-making, and management.

C.5.1.2 Program Management Office (PMO) Support

C.5.1.2.1 Program Management Support

Providing assistance to a Government Program Management Office (PMO). This support could include performing and/or assisting the PMO staff in the development and maintenance of program and project plans, standard operating procedures, contingency plans, continuity of operations, and other documentation. It may also include acquisition support by preparing procurement related documentation, such as Statements of Work, independent Government cost estimates, internal acquisition review board packages and justifications, and source selection material. Financial management support could include the collection and management of financial data; assisting in financial analysis tasks; tracking program progress against the program plan; and preparing required financial reports. PMO support could include Portfolio Management, which would allow DOJ to track and align expenditures across the portfolio in a manner that would dedicate specific investment percentages to broad areas of IT, such as infrastructure, application development and operations, new technology, etc. Other support may include providing meeting support by planning and arranging for meetings, preparing meeting materials and recording and disseminating minutes; development and tracking of correspondence, reports and briefing materials; maintenance of a document library. Support may also include researching and providing recommendations on best practices to improve areas within Program Management; evaluating issues and providing recommendations related to program cost, schedule, and performance; and, providing analysis and recommendations to respond to Congressional, other Government agencies, and industry inquiries; audits; or Congressional testimony.

C.5.1.2.2 Independent Verification and Validation (IV&V)

Processes, procedures and methods that provide an independent monitoring of the development and/or maintenance of IT systems. Software verification and validation (V&V) assists the development organization build quality into the software during the software life cycle. The validation "validates" that the software meets the user's needs, and verification "verifies" that the system is well engineered. Validation includes verification of technical requirements, design, test programs and other program activities to ensure that they are comprehensive, comply with required law, regulations, best practices and industry standards, as well as represent the best solutions to the government's mission and operational requirements. It produces workable solution options to issues, risks, or concerns identified during the verification process. IV&V activities are performed by an agency or a contractor that is not under the control of the organization that is developing the software.

C.5.1.3 System Engineering and Development

C.5.1.3.1 Requirements Analysis

A set of procedures and processes followed by the project team to determine functional and system requirements and their relative importance to users. Users' requirements are documented meaningfully using automated requirements gathering tools such as Rational Rose and UML modeling, wherever applicable. It is assumed that the user knows what he wants, but

has difficulty in translating requirements into data-processing terminology. This procedure helps get the requirements in writing to guide the subsequent efforts of the systems design and implementation. This sub-phase is one of the most important in the entire project life-cycle.

C.5.1.3.2 Joint Requirements Planning (JRP)

JRP consists of workshops with key end-users for planning and designing a system. The users are encouraged to do most of the talking. Information Systems staff members translate what the users want into structured specifications and design so that users can understand and discuss the results. JRP sessions do not contain technical detail. They often involve higher-level managers and sometimes top-management. They establish requirements and justification for a system and the detailed functions it will perform. A major benefit of JRP is making executives think creatively about how information systems can help them. The workshops cause an examination of goals, problems, success factors and strategic opportunities in information strategy planning.

C.5.1.3.3 Joint Applications Development (JAD)

In the JAD session, several knowledgeable people in the subject organization or in the subject functional area meet for extensive and intensive discussions and brain-storming sessions. These sessions are professionally facilitated and discussion/conclusions and disagreements are formally captured and distributed. These sessions strive to accomplish agreement or consensus on the topics of the session. Disagreements are resolved so everyone understands what the target/new process/function/system will and will not accomplish.

C.5.1.3.4 Rapid Applications Development (RAD)

An approach to systems development that incorporates a variety of automated design tools (CASE). RAD focuses on human management and user involvement as much as on technology. RAD aims for rapid development of a single, stand-alone system of limited scope. The use of CASE tools is a necessity for this path, as are rapid development techniques and features such as time-box management, reusability and user workshops. RAD techniques are largely a subset of Systems and Information Engineering techniques.

C.5.1.3.5 Systems and Information Engineering

An integrated set of methodologies and products used to guide and develop information processing within an organization. It starts with enterprise-wide strategic planning and ends with operational applications. It includes activities required for the support of operational systems oriented to enhancing operations of hardware and software systems to include the collection and analysis of systems information, diagnosis of problems and development of recommendations to resolve problems. It establishes and maintains systems and software configuration baseline data and documentation. It includes redesign activities that modify functionality and/or produce technical improvements to enhance software and security. It monitors system execution and performance; tracks and reports change requests (CRs) and discrepancy reports (DRs); performs problem analysis and resolution; and provides technical assistance to the end-user. It performs system and software conversion activities that include the transition of existing applications from one environment to another. It performs production control activities such as the support of cyclical changes to operational workloads, data

compression, data restores, reorganization of files, recovery of systems, production of reports, download/upload of information, and setup and verification of fields and programs for the execution of production runs. It prepares and executes disaster recovery procedures; analyzes, compiles and aggregates data to produce statistical trend analysis reports; develops user-friendly interfaces between different automation functions and upload/download capabilities; and develops and implements an audit strategy to ensure the integrity and confidentiality of data.

C.5.1.3.6 Systems and Database Design

Includes the design approach, alternative designs and analysis, and impact analysis. Maps and maintains traceability of the design to requirements; develops user interfaces; identifies the major components and interfaces of the system; determines impact on work flow processes; and develops testing strategies, test cases and testing plans. Also includes conducting design reviews to clarify design drivers; select an IT platform and/or architecture; identify and weigh portability considerations, potential capacity and performance implications; identify existing systems that may be reused; identify any integration issues with legacy systems; and other pertinent design information. Unique database design tasks include creating the logical and physical database design for a system using data modeling and data normalization techniques.

C.5.1.3.7 Systems Procedures and Standards

Devising systems procedures and standards using all applicable standards and procedures as required by the Federal Information Processing Standards, DOJ requirements, other standards, and the client organization's standards and policies. Includes identifying the applicable standards and procedures and making recommendations about their use to the client organization.

C.5.1.3.8 Systems Development and Testing

Translating system specifications and detailed design documentation into system components, code or both. May include initial development of a prototype of the system that will be tested and evaluated before the systems development effort using automated testing tools, whenever applicable. Includes: developing code, conducting peer reviews and providing summary progress of the development effort; establishing and maintaining the integrity of baseline configuration, software version descriptions and related documentation; establishing test and verification procedures to ensure system integrity so that the system meets functional requirements; and, conducting unit, system and integration testing to validate the system's capabilities. Also includes Performance Testing to verify that the system meets specific response time requirements and User Acceptance Testing to verify that target user groups concur that the business objectives are met.

C.5.1.3.9 Systems Installation and Acceptance

All activities associated with the installation and operation of the system. During systems implementation, includes providing support through the development of prototype installation test plans, installation test reports and the preparation of systems manuals including operations, maintenance and user manuals customized by site. Delivery of the system and all

documentation and products associated with the system. Installation, integration, testing and implementation of the systems developed to include all activities associated with data conversion, data collection, capture, validation, and verification, user training and system turnover.

C.5.1.3.10 Systems Programming

Programs are written using the programming standards established by the client organization. Substantial emphasis is put on a structured process for preparing a test plan, which outlines all of the testing to be done. The programmer plans testing problems thoroughly before the testing begins. The results of the testing are then reviewed by qualified personnel to decide that each program and module is operating satisfactorily.

C.5.1.3.11 Systems Integration

Includes the analysis of the distribution of functionality across systems, development of system interface concepts, designs and specifications, and the development of specifications and standards for information transfer between systems.

C.5.1.3.12 COTS Integration

Includes implementing COTS solutions such as the configuration of COTS database tables, parameters, and interfaces, as well as the design, development and test of Reports, Interfaces, Conversions, Extensions and Forms.

C.5.1.3.13 Interoperability Verification and Testing

Verification and testing to ensure interoperability with existing systems. May include access to existing mainframes and servers, compatibility with operating systems, COTS software and client organization applications, and communications and telecommunications systems.

C.5.1.3.14 Systems Conversion

Converting systems from current environments to new ones including newer evolving/evolved web-based technologies. May include the development of specifications, programming, testing and documentation. Legacy systems may also be selected for the development of new front-end user interfaces. New user interfaces may include web-based or web-enabled front ends.

C.5.1.3.15 Web Development

Includes support services to design, develop, maintain, implement, and document quality electronic publications and applications. It also includes designing electronic publications, databases, and applications in a Unix server environment and assist in the maintenance of servers. Also includes designing multimedia utilizing various applications. Design work is completed within specified legislative and Departmental guidelines. It performs testing on all developed materials documenting results prior to production. Assists staff in development efforts, participate in staff meetings and provide recommendations for solutions to design

problems. Documents all assignments, including applications, procedures and processes. Also includes use of social media, Web 2.0 and other emerging technologies to support transparent and open Government directives. Web 2.0 will allow the design and development of web applications that facilitate interactive information sharing, interoperability, user-centered design, and collaboration. User centered design practices help determine what technologies best meet user needs. Options such as web-based communities, social-networking, video-sharing, wikis, blogs, mash-ups and folksonomies can be leveraged to enhance the user experience.

C.5.1.3.16 Workflow Processing

The use of automated methods for the routing and control of documents and transactions through a process such as procurement requests, personnel requests, etc. Also involves scanning and storing information in digital form on computers. The information may be pictures, drawings or text. This process may also be described as the combining of single work units and their (partial) products as they are aggregated in an overall process, such as data entry to verification to populating a database to query and reporting. It could be represented in a flowchart or a process model where each function is shown with inputs, methods and controls from other functions, outputs to other functions that serve these purposes, and the overall initiating activity and end-product.

C.5.1.3.17 Data Warehousing / Data Mining

Build data warehouses to collect transaction data to allow for easier and faster querying and reporting. Design an environment that allows non-technical personnel to write and maintain queries and reports and/or to provide a means to speed up the writing and maintaining of queries and reports by technical personnel. Simplify the process required to query and report data from multiple systems and/or external sources and/or data stored for query/report purposes only. Build data mining models to allow clients to make better use of the data in their databases. Data mining uses a combination of machine learning, statistical analysis, modeling techniques and database technology to find patterns and subtle relationships in data and infers rules that allow the prediction of future results.

C.5.1.4 Infrastructure Support

C.5.1.4.1 Service Development

The design and development of services and service management processes. Design principles and methods for converting strategic objectives into portfolios of services and service assets. Includes the changes and improvements necessary to increase or maintain value to customers over the lifecycle of services, the continuity of services, achievement of service levels and conformance to standards and regulations. It guides organizations on how to develop design capabilities for Service Management.

C.5.1.4.2 Service Operations

Provisions for effectiveness and efficiency in the delivery and support of services so as to ensure value for the customer and the service provider. Strategic objectives are ultimately realized through Service Operations, therefore making it a critical capability. Maintain stability in Service Operations, allowing for changes in design, scale, scope and service levels. Supporting

operations through new models and architectures such as shared services, utility computing, web services and mobile commerce.

C.5.1.4.3 Service Management

Support for establishing an IT Service Management (ITSM) process intended to align the delivery of information technology (IT) services with needs of the enterprise, emphasizing benefits to customers. Assistance in managing the paradigm shift from managing IT as stacks of individual components to focusing on the delivery of end-to-end services using best practice process models. These services will be based upon the ITIL (Information Technology Infrastructure Library), a globally recognized collection of best practices for information technology (IT) service management. Additional support for ITSM audits based on analysis of four key performance indicators in specific ways:

- (1) Growth and value, which involves tracking revenue growth against investment and utilization.
- (2) Budget adherence, which involves optimizing the use of available funds and avoiding unnecessary expenditures.
- (3) Risk impact, which involves identifying and evaluating the consequences of risks taken or avoided.
- (4) Communication effectiveness, which involves examining internal customer feedback and gauging customer satisfaction and awareness.

C.1.5 IT Security

C.5.1.5.1 Information and Cyber Security

Enhancing IT security of data residing in computer files or during transmission, assessing IT risks relating to privacy, fraud and abuse and the adequacy of internal controls to eliminate and/or mitigate risks to systems being built. Contingency plans cover system failure and recovery procedures. Procedures are developed in case of disaster or other conditions that may severely affect the provision of timely and efficient system services. Includes evaluating and implementing encryption, authenticating users on a system, providing for digital signatures to ensure integrity of electronic messages and files. May include analyzing and maintaining a list of critical systems to decide for each system the time available to transfer to an alternative processing site without significant programmatic impact. Includes systems handling National Security and Limited Official Use (including as a minimum - Law Enforcement Sensitive) data. Also includes the conduct of risk analyses and the development of recommendations and implementations, plans for new procedures and changes to existing systems. Identification and recommendation of new security-related technology product versions and enhancements to existing products and services. Developing implementation, transition and verification testing plans for installing these products within the existing client organization technology infrastructure. Conducting formal Certification & Accreditation (C&A) efforts such as C&A Documentation Preparation and C&A Testing for both legacy and new systems in accordance with all standard security requirements (e.g., DITSCAP, NIACAP, NISPOM, DOJ Directives, etc.). Includes mitigation strategies and mitigation activities for residual risks identified for specific organizations or systems. Development of security policies and procedures and assistance with implementation of these policies. Includes additional service elements for cyber security and privacy protection:

- (1) Provide privacy impact assessments, Personally Identifiable Information (PII) data security, PII monitoring, and mitigation strategies.
- (2) Provide procedures and implementation for intrusion detection, continuous monitoring, risk analysis, and information and cyber security mitigation techniques. Identify potential vulnerabilities to cyber and information security using penetration testing and red teams.
- (3) Provide technologies for identification, modeling, and predictive analysis of cyber threats. Provide the ability for deep analysis of viruses, malicious code, and attack techniques and methods.

C.1.6 Operations and Maintenance

C.5.1.6.1 Systems Enhancements, Support and Maintenance

All requests for system modification and/or enhancements, received after the systems design freeze and after the system is implemented, are classified as planned software maintenance. These requests consist of actions that are important for corrections to the design and future enhancements to the system. Systems support is provided to ensure the successful operation of the system in an accurate, efficient and timely manner. Any necessary fine-tuning and retesting are done following client organization standards and procedures.

C.5.1.6.2 Systems Documentation

Development of all documentation, including manuals, e.g., operations, system maintenance, user and training, and plans, e.g., system integration and site implementation. The document is dynamic in that it will be modified to take advantage of new methodologies, techniques and tools, e.g., CASE. The documentation follows the latest approved standards at the time of development of the system.

C.5.1.6.3 Systems Configuration Management

Systems configuration management activities commence early in the systems development life-cycle and continue for the life of the system. Configuration Management responsibilities include the review of all software, hardware, network and application changes and the identification of potential issues, conflicts or problems relating to the proposed changes, or the timing of the changes. Changes include installation of new products and components, new versions, upgrades, engineering changes, new agency-developed applications and modifications to agency applications. May include the development and implementation of a Configuration Management database and associated plans. Data to be maintained include parameters and configuration information on existing systems, reasons for the changes, associated changes and other items as recommended by the Contractor or required by the client organization. Preparation of reports and briefings to give client organization management recommendations and alternatives.

C.5.1.6.4 User Training

Schedules for implementation are completed, and the users are given their manuals and comprehensive training in the operation of the system. The production files are created or converted to make the system operational. User training may include enterprise security training, other formal instruction on the use of commercially available COTS software, and other techniques such as distance learning and computer based training. Training materials may include web-based training and web-based knowledge management solutions.

C.5.1.6.5 Database Administration

The Database Administrator (DBA) is responsible for database and data dictionary design and establishment, performance monitoring and timing, database reorganization, database backup and recovery, DBMS service utilities, DBMS software maintenance, disk-space management and software planning and evaluation. The DBA is responsible for safekeeping the data and for control of the data and its structure. The DBA is also concerned with the various design methods used in developing databases.

C.5.1.6.6 Technical Refreshment

Identification of aging technology or the technology at risk of becoming obsolete during the life-cycle of a program, and identifying technology refreshment activities required to prevent the decay of the Information Technology infrastructure on which programs are dependent. This will include the identification of specific targets of possible aging technology and recommendation of specific technology to replace it. Recommendations shall include specific timeliness, cost/benefit scenarios and detailed replacement procedures. They may also include the purchase, configuration, installation and operation of the recommended technology as deemed necessary by the government to refresh the aging technology.

C.5.1.6.7 Technology Infusion

Evaluation of an organization's operational use of Information Technology and identification of general and specific areas where current, upcoming or state-of-the-art technology would enhance the organization's operation. This will include identification of the operational components evaluated, specific descriptions of the enhancements possible if the recommended technology were infused into the organization, and specific description of the technology available to realize the enhanced capability. This may also include the purchase, configuration, installation and operation of the recommended technology as deemed required by the government.

C.5.1.6.8 End User Support

Specific areas of support include help desk support, call center support, and a full range of technical support in all areas of computer knowledge. This includes programming, systems design and development, systems analysis and other software tasks. It includes the ability to operate computer systems and associated peripheral equipment including servers, monitors, disk-drives, printers and modems. Support may be requested in mainframe, minicomputer and/or personal computer environments and in field sites. The technical assistance may include database maintenance, performance monitoring and tuning, networking and telecommunications support.

C.5.1.6.9 Field Site Operational Support - (Short and Long-Term)

Provision of IT-skilled personnel permanently in major client organization offices (long-term). Their purpose is to provide assistance to local managers in the performance of various IT functions such as local requirements analysis, systems change requests, implementations, on-the-job training in the use of various COTS hardware and software and in-house developed systems. Generally these personnel will be located in major metropolitan areas but will involve occasional travel (short-term) to smaller, more remote field offices to provide similar services at those offices whose workload cannot justify permanent support.

C.5.1.6.10 Records/Document Management and Information Distribution

Use of automated systems to manage and distribute records and documents. Records management includes, but is not limited to, data entry, tracking, archiving and destruction, reporting and security of paper records through the use of automated tools such as bar-coding. Document management includes, but is not limited to, records management and the use of automated tools to assist in gaining control over revision cycles, tracking revision history, setting user authorizations, redlining, multiple department communications and data-sharing, and storing the metadata about an organization's documents to assist in search and retrieval.

C.5.1.6.11 Data Conversion

Data conversion and migration services to move data between existing client organization systems and between existing and new systems. This could be across operating systems and/or hardware platforms or between different databases. It applies to client organization application files and end-user database files. Activities include creating file inventories, developing procedures for, and conducting, data conversions and ports, and acceptance testing activities. Also includes developing procedures and proposed methods for performing file migration with a minimum disruption to end-users.

C.5.1.6.12 Data Entry

Initialization of data collection processes to capture existing unstructured data to validate data being captured, verify integrity of data collected, and assure all data captured complies with data administration standards. Includes system data dictionaries and documentation to support data collection functions. Personnel may operate keyboard-controlled data entry devices to transcribe data into forms suitable for computer processing. The work requires experience and judgment in searching, interpreting and selecting items from a variety of source documents.

C.5.1.7 Other IT-Related Services

Examples include technical and quality reviews, documentation of existing systems and procedures, preparation of IT standards and procedures, preparation and performance of special presentations, provision of IT training, document analysis, data collection and operational analysis.

C.5.2 Information Systems

C.5.2.1 System Types

Task orders may require SDLC support for virtually any type of information system. It is likely that the following system types will require support under the ITSS-5 contracts:

1. **Infrastructure Systems.** These systems provide the primary infrastructure upon which much of the operational and administrative systems run. Infrastructure systems include basic WAN and LAN routing and switching systems, security systems such as firewalls and intrusion detection/prevention systems, load balancers, virtual resource managers (DNS, IP Addresses, DHCP, etc.), utility services (Time, DNS, Virus Definition distribution, patching, system administration, logging, monitoring, management, common UI administration, etc.), virtual environment/machine management environments, database environments, application hosting environments, common text and video messaging environments, common user/identity repositories, collaboration environments, trouble ticketing systems, file sharing environments and systems and other systems which provide a common infrastructure solution for multiple components and/or agencies.
2. **Administrative Systems.** These systems provide operational support for administrative functions such as procurement tracking, property management, inventory control, etc., and may interface with financial management, human resource, and other types of systems. Also included are Decision Support Systems that retrieve high level information accurately and expeditiously, and are intended to aid managers and executives in making management decisions. Inventory Control systems include the management and tracking of real and other property owned by the user and may involve development, operation, maintenance of systems, application programs and databases associated with inventory management. Property Management systems track data relating to the various aspects of the property in an organization. This serves as a management resource for obtaining timely and accurate data for the status, location, availability, specifications, condition and history of all pieces or sets of property.
3. **Financial Management Systems.** These systems involve the day-to-day tracking of financial allotments, apportionments, budgets, obligations, expenditures, payments, reimbursements, refunds and transfers. They include also the development and provision of data for use in budget formulation and obligation control. Systems or subsystems may include general ledger, disbursements, accounts receivable and payable, purchasing and job cost-accounting.
4. **Human Resource Systems.** These systems involve processing of personnel and payroll actions for various user organizations. The systems also provide data on equal employment opportunity, application tracking, position management, personnel security, and training.
5. **Case Management/Tracking Systems.** These systems provide detailed and aggregate information on cases and matters, summary information on the implementation of Departmental priorities, and operational management information such as stages-of-case-proceedings. These systems also provide summary-level case management

information to meet senior management and administrative needs, and to respond to Congressional and oversight agency queries.

6. Litigation Support Systems. These systems support the litigation of cases involving many documents. They help the legal staff in performing tasks critical to successful litigation including document production, information retrieval, information transfer, information analysis, activity management, and preparation for in court presentations. This support aids attorneys and paralegals in performing generalized legal research, document control, case-file information-handling, and in court presentation before jurors.
7. Law Enforcement Systems. These systems are used to give information, insight and trends concerning law enforcement activities. The systems are developed as tools to help in enforcement activities and collect data from diverse sources (both automated and non-automated systems, public, and Government sources). Enforcement activities are divided into two groups: Intelligence and Operations. Enforcement intelligence groups use Law Enforcement Systems to establish covert criminal trends, establish links between seemingly separate criminal activities, and identify activities of criminal organizations, while Enforcement Operations use these systems to gain information on suspects, gangs, and criminal organizations before and after establishing a case. Law Enforcement Systems are also used to give Law Enforcement Agents information to identify the location and description of a suspect(s), and information necessary to capture a suspect as safely as possible.
8. Geographic Information Systems. These systems extract information from maps, photographs and demographic reports and record it in computer databases. The output products may include statistical reports, maps and graphics that represent statistical relationships, such as bar charts or area maps. The output graphically explains specific conditions, such as population densities or property ownership.
9. Electronic Commerce. These systems support the transfer of documents and business transactions over local and wide area networks (using standard protocols such as X12, X.400 and X.435 and standards being developed by industry and the Federal Government) and the Internet. Electronic Data Interchange and electronic fund transfers are examples of electronic commerce.
10. Video Conferencing. This includes the real-time, two-way transmission of voice and images between two or among more locations.
11. Electronic Document Management. Electronic document management (EDM) systems provide automated tools to electronically organize documents and coordinate their processing for developing, revising, tracking, and distributing documents throughout the life-cycle of the documents. EDM software and services include, but are not limited to, managing/controlling access to information from any source; managing revisions; providing users with efficient information access; automatically taking documents through the review, revision, and approval process; assuring that, as any key information changes, all dependent information changes as well; ensuring users have access to the most recent version of a document as soon as possible; providing the ability to import, assemble, store, and reuse information from any source (data, text, spreadsheets,

graphics, images, CAD, voice, video); and, giving users intelligent access to information from any source for viewing or virtually any computer platform.

12. PMO Support Systems and Tools. These systems provide a collaborative environment for the PMO and associated project teams to manage projects through use of a centralized repository system. Tools will include those which will integrate or track program and project plans from inception through closure such as Project Server and SharePoint, and will be able to provide consolidated reporting or dashboards for tracking and measurement analysis. The document repository system should include features such as version control, change control management, workflows for approvals, feedback, and dispositions.
13. Mash-up Systems. These systems are web-based applications that combine data or functionality from two or more external sources to create a new service. For example, Geographic Information Systems (GIS) could be incorporated with other applications as mash-ups.
14. Mobile Solutions. These systems provide tools and techniques to deliver solutions to a mobile workforce, including solutions working in a connected and disconnected state via mobile devices including mobile computers, personal digital assistants and smart phones.
15. Unified Communications. These systems will be used to consolidate traditionally disparate communication methods (i.e., voice and video) on the data (IP) networks of Components. These systems will integrate real-time communication services such as IP Telephony, presence information, instant messaging, and video conferencing with non real-time communication services such as voicemail, e-mail, and text. These services will allow Components to provide a consistent unified user interface and end user experience across multiple devices and media types. This system will also afford Components the ability to streamline and enhance the functionality of their IT environment while making their user base more efficient and reliable in day-to-day communication.

C.5.2.2 DBMS and Language Types

Task orders may require SDLC support for virtually any type of software application, database management system (DBMS), and language. The tools listed below are representative of the kinds of tools likely to be required to support Work Plan Requests (WPRs). Individual WPRs will identify the specific tools that will be used, including tools beyond this list.

1. Oracle/Oracle Tools
2. Java and Java tools
3. ASP.NET
4. Azure Services Platform
5. Remedy
6. BMC Patrol
7. HP OpenView
8. CiscoWorks and other ACS products
9. Sourcefire

10. Fortinet
11. OpNet
12. Splunk
13. Syslog NG
14. NetFlow
15. VMWare
16. RIMM Blackberry Enterprise server
17. ArcSight
18. Foundstone
19. AppDetective
20. Proofpoint mail gateways
21. iPhone OS 3.x Application SDK
22. Browsers
23. C, C++
24. Microsoft Products:
 1. MS Access
 2. MS SharePoint including MOSS 2007 and beyond
 3. Exchange 2003 / 2007
 4. SQL Server 2008 and beyond
 5. ILM/FIM
 6. SMS, SCCM, SCOM, MOM, all versions
25. Symantec Products: Endpoint protection; Net Backup, SVS
26. Guardian Edge, Credant and other data at rest
27. Applied Identity ID Unify
28. ActiveIdentity middleware and OCSP middleware software for smartcards
29. Pointsec
30. WSUS
31. LanDesk, all modules
32. Sybase
33. DB2
34. Rational Tools
35. HTML, XML
36. SQL Server
37. Web Portals, Web Services, Web 2.0
38. .Net
39. Adobe/PDF and other image file formats, Adobe LiveCycle, Creative Suite
40. Business Objects
41. Siebel
42. ESRI Products
43. PerlScript
44. SAN Technology including NetApp SAN and storage solutions
45. Apache Tools (Tomcat, Struts)
46. Hibernate
47. Nagios

The following are considered legacy DBMS and language types and may require operational support under the ITSS-5 contracts:

1. End-User Personal Computer Software (1-2-3, etc.)

2. Powerbuilder
3. Optimal J
4. Model 204
5. COREL products including Word Perfect Office

C.5.2.3 Computer Environment and Operating Systems

Task orders may require SDLC support for virtually any type of computer environment or operating system.

It is likely the following types and their successors will require support under ITSS-5 contracts:

1. IBM System 390 compatible mainframe computers
2. IBM AS/400
3. Intel compatible microcomputers
4. Unix servers
5. Client/Server (Cooperative computer interaction)
6. Netware (Network Operating System)
7. Windows Server 2008/2012
8. Windows 7
9. Microsoft Office 2007, 2010, and beyond
10. Unix/TCP-IP (Operating systems: Solaris, SCO, HP/UX, AIX, etc.)
11. Thin Client
12. n-Tier
13. VMware
14. Linux (Redhat)
15. Sun Solaris; for server OS Windows 2003/2008; for desktop (2007, 2008, Vista)

The following are considered legacy environments and operating systems and may require operational support under the ITSS-5 contracts:

1. Model Driven Architecture (MDA)
2. Class C2 System (Systems conforming to a C2 level of trust)
3. Windows Server 2000
4. Windows XP/Vista

C.6 Staffing Requirements

(a) The Contractor shall provide only personnel who are fully qualified and competent to perform their assigned work and who possess the basic qualifications for each labor category listed below. In addition to the basic qualifications, the qualifications of personnel assigned to each task performed under this contract shall include the specific expertise required for the performance of the task order.

1. Program Manager
2. Task Manager
3. Project Manager
4. Business Process Engineer

5. Business Systems Analyst
6. Business Consultant
7. Service Delivery Manager
8. Information Services Consultant
9. Enterprise Architect
10. Configuration/Data Management Analyst
11. Information Systems Security Specialist
12. Computer Security Systems Specialist
13. Data Security Specialist
14. Information Systems Security Engineer
15. Cyber Security Specialist
16. Systems Security Architect
17. Systems Engineer
18. Systems Programmer
19. Systems Analyst
20. Software Engineer
21. Programmer Analyst
22. Programmer
23. Management Analyst
24. Integration & Test Engineer
25. Communications Specialist
26. Telecommunications Engineer
27. Network Engineer
28. Network Administrator
29. Quality Assurance Analyst
30. Software Tester
31. IV&V Test Engineer
32. Systems Administrator
33. Database Administrator
34. Web Designer
35. Web Software Developer
36. Web Content Administrator
37. Data Warehousing/Mining Specialist
38. Technical Support Specialist
39. Help Desk Manager
40. Help Desk Specialist
41. Training Specialist
42. Operations/Technical Support Manager
43. Administrative Specialist
44. Technical Writer
45. Graphics Specialist
46. Emerging Technology Specialist
47. Subject Matter Expert
48. Subject Matter Specialist
49. Expert Consultants - Various Disciplines and Skills

(b) U.S. Citizenship Security Clearance Requirements. Each employee of the Contractor providing IT support services under this contract must be a United States citizen and is subject to the DOJ security clearance requirements described in Section H.4. The basic

security provisions in Section H.4 of this solicitation/contract DO NOT cover or call for classified information processing or personnel with clearances above the Sensitive But Unclassified level. However, there is nothing in the contract which restricts client agencies from including such higher level requirements in their individual Work Plan Requests, task order statements of work, or task order statements of objectives for performance based service tasks.

(c) Contractor personnel may be required to travel for extended periods under certain task orders. Such travel is not routinely required.

(d) Note that the DOJ specified labor categories are not intended to cover all of the Contractor's management positions. The Contractor is expected to provide competent overall contract management; this management is not separately billable to the Government, apart from the Program Manager when funded by DOJ under a task order.

(e) Also, the Contractor is required to provide administrative and logistical services as part of its normal business operations and overhead; in most cases these administrative and logistical services are not separately billable. However, if the report is specifically called for as a deliverable under the contract or within a task order, the time expended to prepare such reports is billable at the appropriate hourly rates. The labor categories are not intended to cover these services either. The Contractor shall provide its own facilities, equipment, etc., for management, administrative, and logistical staff; these facilities, equipment, etc. are not separately billable to the Government.

C.7 Government Furnished Property and Equipment

(a) Government Furnished Property (GFP). Any items of GFP, such as office space, to be furnished by the Government will be identified in the Work Plan Request and the specific task order.

(b) Government Furnished Equipment (GFE). Any items of GFE, such as office equipment, desktop workstations, and office supplies to be furnished by the Government will be identified in the Work Plan Request and the specific task order.

(c) The Contractor shall ensure that reasonable measures are taken to safeguard and protect any GFP and GFE from theft, loss, or breakage.

SECTION D – PACKAGING AND MARKING

D.1 Payment of Postage and Fees

All postage and fees related to submitting information to the Contracting Officer or the Contracting Officer's Representative (COR) shall be paid by the Contractor.

D.2 Preservation, Packing and Marking

(a) Preservation, packaging and packing for all items delivered hereunder shall be in accordance with commercial practice and adequate to insure acceptance by common carrier and safe arrival at destination. The Contractor shall place the contract number on or adjacent to the exterior shipping label.

(b) All information submitted to the Contracting Officer or the Contracting Officer's Technical Representative (COTR) shall include the contract number. Each package, report, or other deliverable shall be accompanied by a letter or other document that identifies the deliverable Item Number or Report Requirement that requires the delivered item(s) and indicates whether the Contractor considers the delivered item to be a partial or full satisfaction of the requirement.

SECTION E – INSPECTION AND ACCEPTANCE

E.1 Inspection and Acceptance

(a) Inspection of all support services performed under individual task orders will be performed by the COTR, the Government Task Manager (GTM), or his/her authorized designee(s), at the Government's site, or at the Contractor's site, in accordance with FAR clause 52.246-4 or 52-246-6 (as applicable). Inspection will consist of an examination of the deliverable(s) and/or services for (1) compliance with the statement of work and/or other task order specific requirements, (2) thoroughness with respect to content, and (3) quality with respect to the standards set forth in Section C or the task order.

(b) The Department shall have a minimum of 30 days to inspect and accept items delivered/work performed under the task order. Rejected work and/or comments on all deliverables will be provided to the Contractor by the COTR as specified in the task order. Negative inspection results will be reported immediately to the Contracting Officer. The Contractor shall be responsible for replacement or corrections to the work or deliverable as necessary to meet the standards of acceptance identified in the contract and the task order. The cost to replace or correct nonconforming work or deliverables shall be born as specified in the appropriate Section E.2 clause or as specified in the task order.

(c) The Government will only be responsible for the cost of those corrections ordered above the performance standard specified in the task order.

E.2 FAR Clauses Incorporated by Reference

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this address: <http://www.acquisition.gov/far/>

CLAUSE NO.	DATE	TITLE
52.246-2	Aug 1996	Inspection of Supplies - Fixed Price *
52.246-4	Aug 1996	Inspection of Services – Fixed Price
52.246-6	May 2001	Inspection - Time and Materials and Labor Hour
52.246-16	Apr 1984	Responsibility for Supplies *

* These clauses apply to task orders containing requirements for equipment, software, or supplies. Additional inspection and acceptance requirements for services and supplies may be specified on individual task orders.

SECTION F – DELIVERIES OR PERFORMANCE**F.1 Term of Contract**

The Base Period of Performance shall be from date of award through September 30, 2021. In addition, the contract contains one (1) five-year Option Period that may be exercised at the unilateral discretion of the Government.

F.1.1 Option to Extend the Term of Contract

This contract may be extended, at the option of the Government, at the prices stated in Section B, for a period of five (5) years or fractions thereof by the Contracting Officer giving written notice of the Department's exercise of such option to the Contractor at any time during the term of this contract. Such exercise shall not have effect unless the Contracting Officer has given preliminary written notice of the Department's intent to exercise such option at least thirty (30) days prior to the last day of the term of the contract. Such preliminary notice shall not be construed as an exercise of the option, and will not bind the Department to exercise the option. If the Department exercises such option, the contract period shall commence running on the next day following the expiration of the contract term which was in effect prior to the Department's exercise of such option, and the contract, as extended, shall be deemed to include this option provision; provided, however, that the total duration of this contract, including the exercise of the option under this clause, shall not exceed 120 months after the award date of the contract (see F.1.2 for circumstances allowing an additional six (6) month extension).

F.1.2 Option to Extend Services (NOV 1999) FAR 52.217-8

(a) The Department may require continued performance of any services within the limits and at the rates specified in Section B of this contract under the last year of Option Period 1 (OY1). These rates may not be adjusted. This option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed six (6) months.

(b) The Contracting Officer may exercise this option by giving written notice to the Contractor at any time during the term of this contract.

F.2 Delivery Schedule

This contract requires the delivery of certain reports under Sections C.4.5 and G.3. All other deliverables will be specified on task orders to be issued under this contract.

F.3 Observance of Legal Holidays/Federal Non-Work Days

(a) For work to be performed at Government site(s), the Contractor must establish a standard holiday schedule that exactly coincides with the Government's schedule for employees working on a Government site(s). Holidays observed are listed below. For Government site

work, holidays and other non-work days are not billable unless work is specifically requested by the Government and productive hours are performed on those days. For work to be performed at Contractor site(s), the Holiday schedule may differ if it is customary practice (For example, when the day after Thanksgiving is given in lieu of Columbus or Veterans' Day). The following is a list of the official Federal Government holidays:

- (1) New Year's Day;
- (2) Martin Luther King's Birthday;
- (3) President's Day;
- (4) Memorial Day;
- (5) Independence Day;
- (6) Labor Day;
- (7) Columbus Day;
- (8) Veterans' Day;
- (9) Thanksgiving Day;
- (10) Christmas Day; and
- (11) Inauguration Day (every fourth year for employees working in Washington, D.C.)

(b) No work shall be performed by Contractor personnel on Government facilities on Federal holidays or other non-work days without prior written approval of the COTR. Work performed on holidays, weekends or other non-work days shall be billed at the "One Rate" unit prices as defined in Section B.

(c) There are certain types of irregularly occurring circumstances that prompt the Government to close its offices where Contractor personnel are working, either on a national or local basis (e.g., bomb threats, inclement weather, power outages, death of a national figure, acts of terrorism, or funding lapses). Contractor staff shall not work at Government sites if the Government site is closed, and the Contractor may not bill for hours not worked. However, Contractor staff assigned under the task to work at contractor sites may work and the Contractor may bill for productive hours if the Contractor site is open for business and not affected by the above closure circumstances.

(d) Non-work due to the Government closing its facility(ies) is not an expense directly reimbursable to the Contractor by the Government, since no productive hour of labor was received by the Government. However, nothing in this contract prevents the Contractor from compensating its employees for time not worked during the above circumstances. The Contractor has considered these facts in crafting its overhead rates and policies.

F.4 Notice to the Government of Delays

In the event the Contractor encounters difficulty in meeting performance requirements, or when he anticipates difficulty in complying with the contract delivery schedule or completion date, or whenever the Contractor has knowledge that any actual or potential situation is delaying or threatens to delay the timely performance of this contract, the Contractor shall immediately notify the Contracting Officer and the COTR, in writing, giving pertinent details; provided, however, that this data shall be informational only in character and that this provision shall not be construed as a waiver by the Government of any delivery schedule or date, or any rights or remedies provided by law or under this contract.

F.5 Delivery of Redacted Proposal

Within fifteen (15) days after contract award, the Contractor shall provide the Contracting Officer with a copy of its Technical and Price proposals, as amended, which shall be releasable to the general public in response to Freedom of Information Act (FOIA) requests. The contractor shall assert the appropriate FOIA exception and basis thereof for any material redacted.

F.6 FAR Clauses Incorporated by Reference

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text

available. Also, the full text of a clause may be accessed electronically at this address:

<http://www.acquisition.gov/far/>

CLAUSE NO.	DATE	TITLE
52.242-15	Aug 1989	Stop-Work Order
52.242-17	Apr 1984	Government Delay of Work
52.247-34	Nov 1991	F.O.B. Destination
52.247-35	Apr 1984	F.O.B. Destination, Within Consignee's Premises

The Remainder of This Page Intentionally Left Blank

SECTION G – CONTRACT ADMINISTRATION DATA**G.1 Responsibilities for Contract Administration****G.1.1 Contracting Officer**

(a) The Contracting Officer has the overall responsibility for the administration of this contract. He/she alone, without delegation, is authorized to take actions on behalf of the Government to amend, modify or deviate from the contract terms, conditions, requirements, specifications, details and/or delivery schedules. However, the Contracting Officer may delegate certain other responsibilities to his/her authorized representative.

(b) This contract will be administered by:

Contracting Officer: [To be identified at contract award]
U.S. Department of Justice
Procurement Services Staff
Contract Administration Service
Two Constitution Square, 8th Floor East
145 N Street NE
Washington, DC 20530
Telephone: [To be identified at contract award]

(c) Written communications shall make reference to the contract number and shall be mailed to the above address.

G.1.2 Contracting Officer's Representative (COR) and Government Task Managers (GTMs)

(a) The performance of work required herein shall be subject to the technical direction of the cognizant Contracting Officer's Representative (COR) or assigned Government Task Managers (GTMs), with respect to technical matters pertaining hereto. The GTMs for this contract are specified in each task order award. These persons are qualified and responsible employees of the Government agency for whom the order work is performed. As used herein, "Technical Direction" is direction to the Contractor which fills in details, suggests possible lines of inquiry, or otherwise supplements the scope of work of the contract or task. "Technical Direction" must be confined to the general scope of work set forth herein and shall not constitute a new assignment, nor supersede or modify any other Clause of this contract or task. To be valid, technical direction:

1. must be issued in writing consistent with the general scope of work set forth in the contract or task;
2. shall not change the expressed terms, conditions, or specifications incorporated into this contract or task; and
3. shall not constitute a basis for extension to the contract or task delivery schedule or contract or task price.

(b) The COR or assigned GTMs are authorized to:

1. Act as liaison and to coordinate contractor/government activities;
2. Arrange for and coordinate the use of government resources (personnel, space, documents, etc.);
3. Provide technical guidance in the performance of the contract or task; and
4. Receive, review and approve (but not reject or deny) progress reports, selected invoices and final reports or other functions of a technical nature. The authority to reject performance and deny associated invoices is expressly reserved for the Contracting Officer.

(c) The COR or the assigned GTMs do not have the authority to alter the Contractor's obligations under the contract; direct changes that fall within the purview of the clause entitled "Changes" and/or modify any of the expressed terms, conditions, specifications, or price of the contract or task. If as a result of technical discussions, it is desirable to alter/change contractual obligations or the Specification/Work Statement, the Contracting Officer shall issue such changes in signed correspondence.

(d) The COR assigned cognizance of this contract is:

[To be identified at contract award]
U.S. Department of Justice
Justice Management Division
Service Engineering Staff
Vendor Management
145 N Street NE
Washington, DC 20530
Telephone: [To be identified at contract award]

(e) A copy of all written communications shall be concurrently mailed or otherwise furnished to the Contracting Officer at the address set forth in Section G.1.1.

(f) The Contracting Officer is the only individual who can legally commit or obligate the Government for the expenditure of public funds. The technical administration of this contract shall not be construed to authorize the revision of the terms and conditions of this contract or task. Any such revisions shall be authorized in writing by the Contracting Officer.

G.2 Contractor Representatives

G.2.1 Contract Administration

(a) The Contractor's representative to be contacted for all contract administration matters:

Name: [Offeror to provide this information in its proposal]
Address:

Voice:
Mobile:
Email:

(b) The Contractor's representative shall be responsible for all contract administration issues and shall act as the central point of contact with the Government for all such issues. The representative shall have full authority to act for the Contractor in all contractual matters. The representative shall be able to fluently read, write, and speak the English language.

G.2.2 Program Manager

(a) The Program Manager is:

Name: [Offeror to provide this information in its proposal]
Address:
Voice:
Mobile:
Fax:
Email:

(b) The Program Manager's responsibilities are described in Section C.4.4.1.

G.3 Reports

G.3.1 Tracking/Progress Reports

The various tracking and reporting requirements are set forth in Section C.4.5.

G.4 Payment

G.4.1 General Invoice Requirements

(a) The Contractor shall render original invoices for work performed during the previous month upon successful completion (full or partial) of each requirement, but not more frequently than once per month, to the COTR at the address identified in Section G.1.2. The Contractor shall not combine, on a single invoice, work performed on multiple task orders during a given period.

(b) To constitute a proper invoice, the following information and/or attached documentation shall be included with the invoice (as applicable):

- (1) Name and address of the Contractor;
- (2) Invoice date;
- (3) Contract number;
- (4) Task order number;
- (5) Project number/title;

- (6) Period covered by the invoice;
- (7) CLIN number and description, quantity, unit price and extended total for the period covered;
- (8) Cumulative amounts billed by CLIN to date;
- (9) Shipping and payment terms;
- (10) Name and address of Contractor official to whom payment is to be sent (must be the same as that in the contract or in a proper notice of assignment); and
- (11) Taxpayer Identification Number.

(c) The COTR, after receiving approval from the client organization, will certify the invoice for payment and forward the invoice to the Finance Office specified in paragraph (e) below for payment, and retain for his/her records a copy of each approved/certified invoice. Note: The Government may request the Contractor to submit invoices directly to customer organizations for processing.

(d) Any invoices which are not properly invoiced, or otherwise rejected for services/supplies not received or accepted, will be returned to the Contractor by the COTR with appropriate explanations. The COTR shall notify the Administrative Contracting Officer in these instances.

(e) The office that will make the payments due under this contract (i.e., the designated payment office) is:

U.S. Department of Justice, FDSS
145 N Street NE, Room 7W1004
Washington, DC 20530

(f) All follow-up invoices shall be marked "Duplicate of Original." Contractor questions regarding payment information or check identification should be directed to the DOJ Vendor Assistance Hotline (202) 616-6260.

G.4.2 Fixed-Price Task Orders

The Contractor shall render invoices upon successful completion of each separately priced item in the task order as described in Section G.4.1, but, not more frequently than once per month. This means partial payments for partial deliveries are authorized, per instructions on task orders.

G.4.3 Time-and-Materials or Labor-Hour Task Orders

(a) Payment for work and services rendered under all time-and-materials (T&M) or labor hour (LH) task orders will be made on a monthly basis in accordance with the clause entitled "Payments under Time-and-Materials and Labor-Hour Contracts" (see Section I.1, Clause 52.232-7). In addition to the requirements contained in Section G.4.1, each invoice shall include (as applicable):

- (1) Actual direct labor hours expended by each individual (fractional parts of an hour shall be rounded to the nearest one-fourth (1/4) hour or lesser fraction in

computing the amount payable) multiplied by the appropriate unit price (hourly rate) from the applicable Table B-1 CLIN;

- (2) Itemization of all documented task proposed other direct cost (ODC) items by appropriate Table B-2 CLIN with supporting documentation (including subcontractor/supplier proposals and quotations);
- (3) Itemization of all CLIN X053 actual transportation and per diem expenses being claimed in accordance with Part 31 of the FAR and Section B.5 with supporting documentation. Contractor requests for reimbursement must contain legible copies of individual receipts for all miscellaneous items of \$20.00 value or higher. Each miscellaneous item of less than \$20.00 value (e.g., meals) must be documented but may be included on a mass voucher rather than with individual item receipts; and
- (4) The appropriate Handling Charge Amounts (HCAs) as computed from the Handling Charge Factors, not to exceed the applicable HCF ceilings stated in Section B of the contract.

(b) The COR, after receiving approval from the client organization, will certify the hours worked, ODC items (if any) and satisfactory completion of all work and services billed.

G.4.4 Interest on Overdue Payments

(a) The FAR clause entitled "Prompt Payment" (see Section I.1, Clause 52.232-25) is applicable to payment under this contract and requires interest on overdue payment and improperly taken discounts. Determinations of interest due will be made in accordance with the provisions of the prompt payment clause as modified by paragraph (b) below.

(b) Subdivision (a)(5)(i) of the Prompt Payment clause is modified to specify the following period for constructive acceptance by the Government: The Government agrees to inspect and determine the acceptability of supplies delivered or services rendered in accordance with Section E of this contract. For the purpose of determining the due date for payment and for no other purpose, acceptance will be deemed to occur on the last day of the above stated inspection period. However, the Contractor is not entitled to payment of contract amounts or interest unless and until actual acceptance occurs. If the products are rejected or services deficient, the provisions of this clause will apply to the date the Government receives corrected/replacement products or the date the contractor corrects the deficiencies in services.

G.4.5 Taxpayer Identification Number

The Contractor must include its corporate Tax Identification Number (TIN) and/or its Employer Identification Number (EIN) on each invoice submitted for payment under this contract. This information is required, for example, in order for the Government to comply with the requirement to file Internal Revenue Service Information returns pursuant to the Internal Revenue Code. Invoices received that do not include the required information will be returned to the Contractor without payment. (Note: This information should be entered in the address block on the invoice). Failure to provide a Social Security Number when the Contractor is a sole proprietor or individual may mean that the invoice cannot be processed within the DOJ or

other agency user systems.

G.4.6 FAR Clauses Incorporated by Reference

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es): <http://www.acquisition.gov/far/>

CLAUSE NO.	DATE	TITLE
52.204-7	Apr 2008	Central Contractor Registration
52.232-33	Oct 2003	Payment by Electronic Funds Transfer – Central Contractor Registration

G.5 Pricing of Adjustments

When costs are a factor in any determination of a contract price adjustment pursuant to the "Changes" Clause, or any other clause of this contract, such costs shall be treated in accordance with the contract cost principles and procedures in Part 31 of the Federal Acquisition Regulation in effect on the date of the contract.

G.6 Security Programs Manager (SPM)

(a) Upon contract award, a Security Programs Manager (SPM) will be designated to coordinate those aspects of this contract which pertain to obtaining and maintaining security clearances at the appropriate levels for contractor personnel performing hereunder.

(b) During the pre-award phase of this contract, the SPM is responsible for performing the following duties:

1. Provide the Contracting Officer with the appropriate contractor personnel security screening requirements (including waiver requirements, if appropriate) and background investigation (BI) requirements for obtaining services of non-federal employees under the resultant contract and task orders.
2. Determine the risk level for each contractor position. The risk level must be based on an overall assessment of the damage that an untrustworthy contractor could cause to the efficiency or the integrity of Departmental operations. The SPM shall provide this information to the Contracting Officer for inclusion in the resultant contract.
3. Certify that the personnel security requirements of the contract are adequate to ensure the security of Departmental operations, information and personnel. The SPM shall provide this written certification to the Contracting Officer prior to release of the Request for Proposals.

(c) The SPM for this contract is (to be filled in by the Contracting Officer upon contract award):

(Component Name)
U.S. Department of Justice

Telephone: _____

(d) The personnel security requirements of this contract are set forth in the Sections C.4.4.4 and H.4 of this contract

(e) Following award of this contract, the SPM shall ensure that the personnel security requirements set forth herein are followed. In addition, the SPM shall comply with the supplemental guidelines provided to him or her by the Contracting Officer.

The Remainder of This Page Intentionally Left Blank

SECTION H – SPECIAL CONTRACT REQUIREMENTS

H.1 Ordering

H.1.1 General

(a) Any supplies and services to be furnished under the ITSS-5 contracts shall be ordered or confirmed by the placement of task orders by the Procurement Services Staff (PSS) Administrative Contracting Officer (ACO) set forth in Section G. No other individuals are authorized to place orders. Such orders may be issued anytime during the term of this contract (see Section F.1). Task orders may be issued orally, in writing (paper) or by electronic commerce methods. All oral orders must be confirmed in writing.

(b) Only the Justice Management Division, Procurement Services Staff, is authorized to place orders with the Contractor(s).

(c) The Contractor shall not proceed with any work under a proposed task order unless authorized by the Contracting Officer. All task orders are subject to the terms and conditions of this contract. In the event of a conflict between a task order and this contract, the contract shall control.

(d) Any order issued during the effective period of the contract and not completed within that period shall be completed by the Contractor within the time specified in the order. In no event shall the completion date for any task order extend for a period of more than 183 days (i.e. six months) beyond the expiration date of the contract, unless as authorized in writing by the ACO. [For example, when a “completion” style task order required more than the 183 days to complete the work.] In such instances, the contract shall govern the Contractor's and Government's rights and obligations with respect to that order to the same extent as if the order were completed during the contract's effective period.

(e) Funds for other than the minimum guarantee will be obligated by each task order.

(f) There are no minimum or maximum dollar amount limitations for individual task orders placed under the ITSS contracts. The (cumulative) ceiling amount of all orders placed under the ITSS-5 contracts is specified in Section B.2. Each task order issued hereunder will contain a dollar ceiling which the contractor shall not exceed except at its own risk.

(g) If mailed, a task order is considered “issued” when the Government deposits the order in the mail. Orders may be issued orally, by facsimile, or by electronic commerce methods by the authorized PSS Contracting Officer.

(h) Since multiple awards will be made, after meeting the minimum guarantee requirement for each contract (see Section B.2), determinations as to which contractor(s) will receive individual task orders will be at the sole discretion of the Government following the procedures set forth in H.1.2 below. Such determinations will be made on the basis of what is in the best interests of the Government, taking into account factors such as availability and suitability of contractor resources, quality of contractor past performance, and price.

H.1.2 Fair Opportunity Competitions

(a) The ITSS-5 contracts include two (2) distinct competitive tracks; a Small Business Track which is eligible for all task orders; and an Unrestricted Track which is eligible to compete for task orders issued on an unrestricted basis. The task order CO shall determine to conduct the procurement on either an unrestricted basis for competition between prime contractors from both the large and small business pool or as a small business set-aside in which competition will be limited to only those prime contractors in the small business pool. The Task Order solicitation will notify Offerors if a set-aside will be used. The CO may issue a request for capabilities statement to the small businesses for task orders that are determined to be potential candidates for small business set-aside. Small business contractors will be required to demonstrate their capabilities to meet all functional requirements of task including the complexity of task, size of task, and the associated staffing plan. Small business contractors will be required to propose to provide at least 50% of the services to be provided, and must describe which SOW services they intend to provide through the use of their own employees, and which SOW services their subcontractors intend to provide, and be evaluated accordingly as a team. Small business proposals that, in the judgment of the CO do not allow for a “meaningful” portion of the services to be provided by employees of that business concern will not be eligible for task order award. Pass-thru’s or other brokerage style arrangements are not permitted. Ordinarily a minimum of two (2) small businesses must meet the evaluation criteria established by the Government for the task order to be set-aside for competition in the small business pool.

(a) The Department intends to compete each task order to the maximum extent practicable by issuing a Work Plan Request (see Section C.4.2) to each ITSS-5 Contractor subject to the eligibility requirement in paragraph (a) above. The only exceptions to this method of consideration are:

- (1) The agency need for the supplies or services is so urgent and compelling that providing the opportunity would result in unacceptable delays;
- (2) Only one contractor is capable of providing the supplies or services at the level of quality required because the supplies or services are unique or highly specialized;
- (3) The order should be placed on a sole-source basis in the interest of economy and efficiency as a logical follow-on to an order already issued under the contract, provided that all eligible ITSS-4 Contractors were given a fair opportunity to be considered for the original order; or
- (4) It is necessary to place an order to satisfy a minimum guarantee.

(b) The Department may use oral proposals and streamlined procedures, in lieu of requesting a written proposal when placing a task order. In such instances the Contracting Officer will exercise broad discretion in ensuring that each ITSS-5 Contractor is provided a fair opportunity to be considered for the order.

(c) The ITSS-5 contractors are encouraged to bid on the maximum numbers of WPRs to

enhance competition. While there is no minimum WPR response rate, the Contracting Officer will consider the Contractors' response rate (to WPRs) when exercising the option period of the Basic Contract.

(e) No protest under FAR Subpart 33.1 for task orders under \$10M is authorized in connection with the issuance or proposed issuance of a task order under the ITSS-5 contracts except for a protest on the grounds that the order increases the scope, period, or maximum value of the ITSS-5 contracts.

H.1.3 Task Order Performance

For task orders issued on a time-and-material or labor-hour basis, the Government shall not be obligated to pay the Contractor any amount in excess of the total (ceiling) price identified in the task order, and the Contractor shall not be obligated to continue performance if to do so would exceed the applicable ceiling price, unless and until the Contracting Officer has notified the Contractor, in writing, that the applicable ceiling price has been increased and shall have specified in the notice a revised ceiling that shall constitute the ceiling price for performance under the task order (see Section I.1, clause 52.232-7 for the Contractor's notification responsibilities to the Government as it accrues costs reaching 85% of the then current task ceiling).

H.1.4 Performance Incentive Awards

(a) The Department may, at its option, include provisions for a Performance Incentive Award (PIA) in any Work Plan Request issued under the ITSS-5 contracts. The purpose of a PIA is to provide additional incentive for the Contractor to perform at a high quality level on a particular task order. The purpose of this section is to establish a general framework for the PIA and not to establish specific evaluation criteria or weights.

(b) For those task orders where a PIA is to be considered by the client agency, a Performance Incentive Plan (PIP) will be issued with the WPR. The PIP will contain the definition of the PIA periods, the maximum PIA percentage, and (when the Task Order is placed under contract) the total PIA amount and the allocation of that amount to the PIA periods. The procedures and criteria contained in the PIP may be changed unilaterally by the Contracting Officer no later than fifteen (15) calendar days after the start of the relevant PIA period. Any such alterations shall not change the total available PIA potential for the task order nor change the PIA earned by the Contractor in any completed PIP period.

H.1.5 Task Order Evaluation Reports

(a) The Department will require the client agency to prepare a formal evaluation report on and assign a performance rating to the Contractor's performance of each task order or group of task orders. For on-going, long term task orders, these reports may be done on an annual or more frequent basis. These reports will be made available to the Contractor in accordance with FAR Section 42.15.

(b) The reports will be considered in the Department's unilateral exercise of option year renewals (see Section F.1.1), and when placing additional task orders. The Department will make available the evaluation reports to Federal agencies seeking past performance

information on the Contractor as part of a Federal contract procurement.

H.1.6 Release of Claims

After completing each task order, and prior to final payment, the Contractor shall furnish to the Contracting Officer, a release of claims against the United States arising out of the task order, other than claims specifically excepted from the operation of the release. Copies of the required form may be obtained from the Contracting Officer at the address listed in Section G.1.2.

H.1.7 Agency Task Order Ombudsman

The designated agency Task Order Ombudsman for IDIQ type contracts awarded by the Department of Justice, Procurement Services Staff is:

TBD
Department of Justice
Procurement Policy and Review Group
Management and Planning Staff
145 N Street NE Room TBD
Washington DC 20530

Telephone: (202)
Facsimile: (202)
Email: @usdoj.gov

Upon request(s), the above individual will review complaints from contractors and ensure they are afforded a fair opportunity to be considered for award of task orders consistent with the procedures in the contract.

H.2 Data and Property Rights

(a) Government Furnished Data and Materials. The Government shall retain all rights and privileges, including those of patent and copy, to all Government furnished data. The Contractor shall neither retain nor reproduce for private or commercial use any information or other materials furnished or made available under this contract (to include task orders issued under this contract). The Contractor agrees not to assert any rights at common law or in equity or establish any claim to statutory copyright in such data. These rights are not exclusive and are in addition to any other rights and remedies to which the Government is otherwise entitled elsewhere in this contract or the task order.

(b) Contractor Produced Data and Materials. All property rights, including publication rights, in the information and materials first produced by the Contractor in connection with this contract (to include task orders issued under this contract) shall vest in the Government. Information and materials shall include, but are not limited to: computer software applications/data bases, software documentation, plans, systems analyses, reports, extracts, test data and procedures.

(c) Commercial Computer Software. At a minimum, the rights of the Government regarding the use, reproduction and disclosure of commercial computer software provided under a task order shall be as described in Section I.1, FAR Clause 52.227-19. Additional rights may be specified by the Government in the WPR and/or task order.

H.3 Organizational Conflict of Interest

(a) At the individual task order level, the Contractor will be required to warrant that, to the best of its knowledge and belief, and except as otherwise set forth in this contract or the task order, it does not have any organizational conflict of interest as defined below.

The term "organizational conflict of interest" means a situation where a Contractor has interests, either due to its other activities or its relationships with other organizations, which place it in a position that may be unsatisfactory or unfavorable (a) from the Government's standpoint in being able to secure impartial, technically sound, objective assistance and advice from the Contractor, or in securing the advantages of adequate competition in its procurement; or (b) from industry's standpoint in that unfair competitive advantages may accrue to the Contractor in question.

(b) The Contractor agrees that, if after placement of a task order it discovers an organizational conflict of interest with respect to the task order, the Contractor shall make an immediate and full disclosure in writing to the Contracting Officer that shall include a description of the action that the Contractor has taken or proposes to take to avoid, eliminate or neutralize the conflict. The Department may, however, terminate the task order for the convenience of the Government if it would be in the best interest of the Government.

(c) If the Contractor was aware of organizational conflict of interest before the placement of a task order and intentionally did not disclose the conflict to the Contracting Officer, the Department may terminate the task order at no cost to the Government.

H.4 Personnel Security Requirements

H.4.1 The work to be performed under this contract will involve access to unclassified information. All references to "contract(or) personnel" and "contract employee" in this clause include all individuals that will perform under this contract, including individuals employed by the Contractor, team member, subcontractor, consultant, and/or independent Contractor.

H.4.2 Duplication or disclosure of the data and other information to which the Contractor may have access as a result of this contract is prohibited by Public Law and is subject to criminal penalties.

H.4.3 Contractor Personnel

- A. All Contractor personnel will be subject to a Public Trust Investigation (PTI). Except where specifically noted otherwise, the Government will be responsible for conducting the investigation and the cost of the investigation. All investigations will be conducted in accordance with applicable Executive Orders, DOJ Orders, Office of Personnel

Management (OPM) guidance, Homeland Security Presidential Directive 12 (HSPD-12), and Federal Information Processing Standard Publication 201 (FIPS 201).

- B. PTI certifications will be accepted from other Federal agencies provided the investigation performed by the other agency meets or exceeds DOJ requirements.
- C. The Contractor will not be permitted to commence performance under this contract until a sufficient number of its personnel, as determined by the COR and Security Programs Manager (SPM), have received the requisite security approval.
- D. During the life of the contract, the Contractor shall ensure that no contract employee commences performance hereunder prior to receipt of a written authorization from the Contracting Officer, the COR, or the SPM.

H.4.4 Access to Unclassified Information

Contractor personnel requiring access to unclassified information will fall under the following categories:

1. High Risk. High risk positions are those positions that have the potential for exceptionally serious impact on the integrity and efficiency of the DOJ and involve duties especially critical to the DOJ or a program mission with broad scope of policy or program authority.
2. Moderate Risk. Moderate risk positions are those positions that have the potential for moderate to serious impact on the integrity and efficiency of the DOJ. Duties involved are very important to the DOJ or program mission with significant program responsibility or delivery of services.
3. Low Risk. Low Risk positions are those positions that have limited potential for adversely affecting the national security operations of the Department.

H.4.5 Pre-Appointment Background Investigations and Waivers

- A. Background investigations must be conducted and favorably adjudicated for each contract employee prior to commencing work on this contract. However, where programmatic needs do not permit the Government to wait for completion of the entire background investigation, a pre-appointment background investigation waiver can be granted by the SPM, in consultation with the cognizant COR. The extent of the background investigation will vary depending upon the Risk Category associated with each position and whether each position is long- or short-term. Short-term is defined as contract employees having access to Federally-controlled information systems and/or unescorted access to Federally-controlled facilities or space for six months or fewer. The requisite background investigation does not need to be initiated for short-term positions as part of the pre-employment waiver except in the case of non-U.S. citizen contract employees. However, long-term contract employees requiring unescorted access to Federally-controlled facilities and/or access to any Federally-controlled information system shall be subject to the requisite background investigations described below. A waiver will be disapproved if it develops derogatory information that cannot be resolved in the contract employee's favor. When a waiver has been disapproved, the COR, in consultation with the SPM, will determine (1) whether the contract employee will no longer be considered for work on a DOJ contract or (2) whether to wait for the completion and favorable adjudication of the background investigation before the contract employee commences work on a Department contract. The minimum pre-appointment investigative requirements are as follows:

1. High Risk Positions. The minimum background investigation required is a five year scope Background Investigation (BI), and the five year reinvestigation required is an Access National Agency Check with Inquiries (ANACI). The Standard Form (SF) 85P, Questionnaire for Public Trust Positions, is required.
 2. Moderate Risk Positions. The minimum background investigation required is a Minimum Background Investigation (MBI) for “moderate” impact on the integrity and efficiency of the DOJ or a Limited Background Investigation (LBI) for “serious” impact potential on the DOJ’s integrity and efficiency. The five year reinvestigation required is a National Agency Check with Law and Credit (NACLC). The SF-85P is required.
 3. Low Risk/Non-Sensitive Positions. The minimum background investigation required for Low Risk/Non-Sensitive positions is a National Agency Check with Written Inquiries (NACI) and the required five year reinvestigation is also a NACI. The SF-85, Questionnaire for Non-Sensitive Positions, is required.
- B. The pre-appointment background investigation waiver requirements include:
1. Favorable review of the security questionnaire form;
 2. Favorable FBI fingerprint results;
 3. Verification of citizenship (copy of a birth certificate, Naturalization Certificate, or U.S. Passport);
 4. Verification of compliance with the DOJ residency requirement;
 5. Favorable credit report for contract personnel in High Risk and Moderate Risk positions; and,
 6. Verification of the initiation of the appropriate background investigation for long-term Contractor personnel.

H.4.6 Required Security Forms

- A. The following forms must be completed and submitted by the Contractor’s Corporate Security Officer for each contract employee PTI:
1. FD-258 Applicant Fingerprint Card. Two sets are required per applicant. The Contractor may schedule appointments with the SPM to be digitally fingerprinted; otherwise, fingerprinting by the FBI is required. All pertinent information must be completed by the individual taking the prints, or by the FBI if prints are taken there.
 2. SF-85 Questionnaire for Non-Sensitive Positions -or- SF-85P Questionnaire for Public Trust Positions. The contract employee shall complete the SF-85/SF-85P via the Electronic Security Questionnaires for Investigations Processing (e-QIP) System after first obtaining access to e-QIP from the SPM (see paragraph (C) below). The Contractor shall also submit a hard copy of the form (as completed and signed by the contract employee) with the remainder of the security package.
 3. DOJ-555 Fair Credit Reporting Act Disclosure. Authorizes DOJ to obtain one or more consumer/credit reports on the individual. This is required for Contractor personnel in High Risk and Moderate Risk positions.
 4. Foreign National Relatives and Associates Statement. This is only required if any relatives listed on the SF-85/SF-85P are foreign nationals.

5. Confidentiality Agreement for Contractor and Subcontractor Employee. Refer to the section entitled, "Security of Department Information and Systems," for confidentiality requirements.
- B. The Contractor shall also submit a credit report for each individual designated at the High Risk or Moderate Risk level, and have resolved satisfactorily any individual credit issues.
- C. Using e-QIP. Immediately after contract award, the Contractor shall designate an employee as its "e-QIP Initiator" and provide the name of this person to the COR. The e-QIP Initiator must have, at a minimum, a favorably adjudicated MBI and the appropriate DOJ security approval before being given access to e-QIP. After the e-QIP Initiator's security approval is granted, the Contractor will be configured in e-QIP as a sub-agency to DOJ. The Contractor will then be responsible for initiating all contract personnel in e-QIP for completion of the security questionnaire form and forwarding the electronic form along with a hard copy of the form (as completed and signed by the contract employee) with the remainder of the security package to the designated DOJ representative. Subject to the prior approval of the SPM, the Contractor may designate an e-QIP Initiator for each subcontractor. Subcontractor e-QIP Initiators must have, at a minimum, a favorably adjudicated MBI and the appropriate DOJ security approval before being given access to e-QIP.

H.4.7 Citizenship and Residency Requirements

- A. Residency Requirement. Contract employees, both United States (U.S.) citizens and non-U.S. citizens, must meet the Department's Residency Requirement, i.e., he/she must have lived in the U.S. three of the last five years immediately prior to employment under the Department contract; and/or worked for the U.S. overseas in a Federal or military capacity; and/or be a dependent of a Federal or military employee serving overseas. At the Department's sole discretion, the residency requirement may be waived by the Department Security Officer (DSO) on a case-by-case basis where justified by extenuating circumstances.
- B. Citizenship. The DOJ gives strong priority to contract employees that are U.S. citizens and nationals. Any prospective contract employee that is a foreign national must be from a country allied with the U.S. (see <http://www.state.gov/s/l/treaty/collectivedefense/>). At the Department's sole discretion, a waiver of the allied nations list requirement may be granted by the DSO on a case-by-case basis where justified by extenuating circumstances. The Contractor is responsible for verifying that all non-U.S. citizens working under this contract have been lawfully admitted to the U.S. Contract employees requiring access to DOJ Information Technology (IT) resources are subject to the following additional restriction:

Non-U.S. citizens are not authorized access to or permitted to assist in the development, operation, management or maintenance of DOJ IT systems unless a waiver has been granted by the Head of the DOJ component, with the concurrence of the DSO and the DOJ Chief Information Officer (CIO). Such a waiver will be granted only in exceptional and unique circumstances. It should be noted that the Justice Consolidated Office Network (JCON) is a sensitive "DOJ IT system" and any contract employee that will need access to JCON must be a U.S. citizen or have received a waiver.
- C. Dual Citizenship. U.S. citizens who hold dual citizenship with a foreign country may be considered for contract employment. However, how the contract employee obtained or

exercises his or her dual citizenship status will be a consideration in the adjudication process.

H.4.8 Procedures for Pre-Screening Applicants and Investigation

- A. The Contractor shall perform the following pre-screening and investigation duties for all persons proposed for work under this contract:
1. Furnish to each proposed contract employee the forms described in Section 5.6 above and ensure that adequate instructions for completing the forms are provided to each applicant.
 2. Ensure that applicants obtain two (2) complete sets of their fingerprints on the prescribed Form FD-258 from an organization qualified to take fingerprints.
 3. Collect completed forms from each applicant and review all forms for completeness and correctness. This includes, for example, satisfactory resolution of address issues or discrepancies. Return any incomplete or incorrect form(s) to applicant(s) to be corrected and re-submitted.
 4. Submit completed forms to the COR by no later than (14) calendar days after receipt of the blank forms and access to e-QIP has been initiated.
 5. As directed by the COR, initiate pre-appointment waivers for certain positions. This may entail performing credit history checks and submission of these checks as part of the security package, including satisfactory resolution of any issues prior to submission to the Government.
 6. As directed by the COR, review all forms prior to their being submitted to DOJ to ensure that candidates meet DOJ requirements, including residency and citizenship requirements.
- B. The Department will be responsible for the following:
1. Determine the appropriate risk level for each contract employee position.
 2. Provide the Contractor an adequate supply of forms and instructions for completing the forms within five business days after contract award. Ensure that the Contractor is provided access to the e-QIP system.
 3. Ensure that completed security forms are forwarded to the appropriate investigating agency in accordance with appropriate internal procedures. The investigating agency will conduct the requisite investigations.
 4. Determine whether pre-appointment background investigation waivers will be needed, and if so, which positions will require such waivers. The COR will notify the Contractor which pre-appointment waivers to initiate.
 5. Notify the Contractor of the results of background investigations as they are completed and adjudicated. The COR will notify the Contractor of any applicants who are found ineligible for employment security approval so that the Contractor can immediately recruit and initiate paperwork to clear replacement applicants.
 6. Notify the Contracting Officer when a sufficient number of contract employees have received employment security approvals or pre-appointment waivers approvals. Upon receipt of this information and any other information which may be required

elsewhere in the contract, the Contracting Officer will issue the Contractor a Notice to Proceed which permits the commencement of work under the contract.

7. Maintain an up-to-date file of Certificates of Investigation (COI) and other background investigation-related documentation for all contract employees throughout the life of the contract.
- C. The investigating agency will furnish the relevant SPM the results of each proposed contract employee's investigation through issuance of a Certificate of Investigation (COI). Upon receipt of the COI and any other pertinent documents from the investigating agency, the SPM will determine whether or not each proposed contract employee should be granted employment security approval. This decision process is called "adjudication." The SPM will notify, if required, the investigating agency of the adjudicative determination of each investigation. If OPM is the investigating agency, this will be accomplished by the SPM completing and submitting to OPM an INV Form 79A, "Report of Agency Adjudicative Action."

H.4.9 Identity Proofing and Badging

- A. During the life of this contract, the right to unescorted access to Federally-controlled facilities and/or access Federally-controlled information systems shall be made available after the contract employees have (1) met the identity proofing requirements outlined below, and (2) completed all other security requirements stated elsewhere in this contract. During all operations on Government premises, the contract employees shall comply with the rules and regulations governing the conduct of personnel and the operation of the facility. The Government reserves the right to require contract employees to "sign-in" upon entry and "sign-out" upon departure from the DOJ facility.
- B. All contract employees requiring unescorted access to Federally-controlled facilities and/or access to Federally-controlled information systems (regardless of whether they will be issued a DOJ badge), shall comply with the identity proofing and registration requirements outlined below:
1. Contract employees must present two forms of identification in original form prior to commencement of work under this contract and badge issuance (acceptable documents are listed in Form I-9, OMB No. 1615-0047, "Employment Eligibility Verification," and at least one document must be a valid State or Federal Government-issued picture ID); and,
 2. Contract employees must appear in person at least once before a DOJ official who is responsible for checking the identification documents. This identity proofing must be completed prior to commencement of work under this contract and badge issuance (as applicable), and must be documented by the DOJ official.
- C. All contract employees requiring unescorted access to a DOJ controlled facility shall comply with the badge requirements outlined below:
1. When any Contractor employees enter a DOJ building for the first time, the contract employees shall allow one hour for security processing and the fabrication of buildings access badges.
 2. Building access badges shall be subject to periodic review by the Contractor's Supervisor and checked against the employee's personal identification. The contract employees shall present themselves for the issuance of renewed badges when

required by the Government as scheduled by the COR or his designee. The Contractor shall notify the COR when employee badges are lost, and must immediately apply for reissuance of a replacement badge. The Contractor shall pay for reissued building access badges. It is the Contractor's responsibility to return badges to the COR or his designee when a contract employee is dismissed, terminated or assigned to duties not within the scope of this contract.

H.4.10 Replacement Personnel

- A. Security investigations are very costly to the Government. The Contractor shall make every effort to preclude incurrence of costs by the Government for security investigations for replacement of employees, and in so doing, shall assure that otherwise satisfactory and physically able employees assigned hereunder remain in contract performance for at least one (1) year. The Contractor shall take all necessary steps to assure that Contractor personnel who are selected for assignment to this contract are professionally qualified and personally reliable, of reputable background and sound character, and meet all other requirements stipulated herein.
- B. The fact that the Government performs security investigations shall not in any manner relieve the Contractor of its responsibility to assure that all personnel furnished are reliable and of reputable background and sound character. Should a security investigation conducted by the Government render ineligible a Contractor furnished employee, the Contracting Officer will investigate the cause and determine whether the Contractor has abdicated its responsibilities to make every effort to select reliable employees of reputable background and sound character. Should there be need to replace a contract employee due to nonperformance, the Contracting Officer will determine whether the Contractor has abdicated its responsibilities to make every effort to select trained and experienced employees.
- C. Should the Contracting Officer determine that the Contractor has failed to comply with these terms, the Contractor may be held monetarily responsible, at a minimum, for all reasonable and necessary costs incurred by the Government to (a) provide coverage (performance) through assignment of individuals employed by the Government or third parties in those cases where absence of Contractor personnel would cause either a security threat or DOJ program disruption and (b) conduct security investigations in excess of those which would otherwise be required.
- D. Nothing in this Clause shall require the Contractor to bear costs involved in the conduct of security investigations for replacement of an employee who becomes deceased or severely ill for a long period of time.
- E. Acceptance by the Government of consideration to which the Government may be entitled pursuant to paragraph (c) above shall not be construed to establish a course of conduct which will serve to limit the rights and remedies otherwise available to the Government. Under no circumstances shall the Contractor fail to comply with the terms and conditions set forth herein without assuming liability for such failure as may be established pursuant to this Clause. The rights and remedies conferred upon the Government by this Clause are in addition to all and other rights and remedies specified elsewhere in this contract or established by law.

H.4.11 Contractor Facility

The Contractor shall implement physical controls as necessary to maintain the integrity and confidentiality of all data/information in its possession. At a minimum, the following requirements shall be in effect for Contractor controlled spaces where information is processed and/or stored:

1. Access to the facility shall be limited to Contractor personnel or those escorted by Contractor personnel.
2. Document/media storage areas shall be restricted to persons requiring access to them on a need-to-know basis and have a security access approval granted by the Department.
3. All designated storage areas/containers shall be made available for inspection upon initial award of a contract and semiannually or as otherwise directed by the Security Programs Manager, Contracting Officer Representative or Contracting Officer Representative's designee.
4. When Grand Jury information is in actual use by authorized personnel, it shall be protected as follows:
 - a. Kept under constant review by an authorized person who is in a physical position to exercise direct security controls over the material;
 - b. Covered, turned face down, placed in storage containers, or otherwise protected when unauthorized persons are present;
 - c. The room containing the materials shall be locked when vacated for short periods of time; and
 - d. Returned to storage containers/areas as soon as practical after use.

H.5 Security of Department Information and Systems

Applicability of Contractor and Subcontractors

This clause applies to Contractor, all subcontractors, including any cloud service provider ("CSP"), and personnel of Contractor, subcontractors, and CSPs (hereinafter collectively, "Contractor") that may access, retrieve, process, store, transmit, or dispose of DOJ Information. It establishes and implements specific DOJ requirements applicable to this Contract. The requirements established herein are in addition to those included in the Federal Acquisition Regulation ("FAR"), including FAR 11.002(g) and 52.239-1, the Privacy Act of 1974, and any other applicable laws, mandates, or Executive Orders pertaining to the development and operation of Information Systems and the protection of Government Information. This clause does not alter or diminish any existing rights, obligation or liability under any other civil and/or criminal law, rule, regulation or mandate.

General Definitions

The following general definitions apply to this clause. Specific definitions also apply as set forth in other paragraphs.

- A. **Information** means any communication or representation of knowledge such as facts, data, or opinions, in any form or medium, including textual, numerical, graphic, cartographic, narrative, or audiovisual. Information includes information in an electronic

format that allows it be stored, retrieved or transmitted, also referred to as “data,” and “personally identifiable information,” (“PII”), regardless of form.

- B. **Personally Identifiable Information (or PII)** means any information about an individual maintained by an agency, including, but not limited to, information related to education, financial transactions, medical history, and criminal or employment history and information, which can be used to distinguish or trace an individual's identity, such as his or her name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.
- C. **DOJ Information** means any Information that is owned, produced, controlled, protected by, or otherwise within the custody or responsibility of the DOJ, including, without limitation, Information related to DOJ programs or personnel. It includes, without limitation, Information (1) provided by or generated for the DOJ, (2) managed or acquired by Contractor for the DOJ in connection with the performance of the contract, and/or (3) acquired in order to perform the contract.
- D. **Information System** means any resources, or set of resources organized for the accessing, collecting, storing, processing, maintaining, using, sharing, retrieving, disseminating, transmitting, or disposing of (hereinafter collectively, “processing, storing, or transmitting”) Information.
- E. **Covered Information System** means any information system used for, involved with, or allowing, the processing, storing, or transmitting of DOJ Information.

Confidentiality and Non-disclosure of DOJ Information

- A. Preliminary and final deliverables and all associated working papers and material generated by Contractor containing DOJ information are the property of the U.S. Government and must be submitted to the Contracting Officer (“CO”) or the CO's Representative (“COR”) at the conclusion of the contract. The U.S. Government has unlimited data rights to all such deliverables and associated working papers and materials in accordance with FAR 52.227-14.
- B. All documents produced in the performance of this contract containing DOJ Information are the property of the U.S. Government and Contractor shall neither reproduce nor release to any third-party at any time, including during or at expiration or termination of the contract without the prior written permission of the CO.
- C. Any DOJ Information made available to Contractor under this contract shall be used only for the purpose of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of this contract. In performance of this contract, Contractor assumes responsibility for protection of the confidentiality of any and all DOJ Information processed, stored or transmitted by the Contractor. When requested by the CO (typically no more than annually), Contractor shall provide a report to the CO identifying, to the best of Contractor's knowledge and belief, the type, amount, and level of sensitivity of the DOJ Information processed, stored, or transmitted under the contract, including an estimate of the number of individuals for whom PII has been processed, stored or transmitted under the contract and whether such information includes social security numbers (in whole or in part).

Compliance with Information Technology Security Policies, Procedures, and Requirements

- A. For all Covered Information Systems, Contractor shall comply with all security requirements, including but not limited to the regulations and guidance found in the Federal Information Security Management Act of 2014 ("FISMA"), Privacy Act of 1974, E-Government Act of 2002, National Institute of Standards and Technology ("NIST") Special Publications ("SP"), including but not limited to NIST SP 800-37, 800-53, and 800-60 Volumes I and II, Federal Information Processing Standards ("FIPS") Publications 140-2, 199, and 200, OMB Memoranda, Federal Risk and Authorization Management Program ("FedRAMP"), DOJ IT Security Standards, including DOJ Order 2640.2, as amended. These requirements include, but are not limited to:
1. Limiting access to DOJ Information and Covered Information Systems to authorized users and to transactions and functions that authorized users are permitted to exercise;
 2. Providing security awareness training including, but not limited to, recognizing and reporting potential indicators of insider threats to users and managers of DOJ Information and Covered Information Systems;
 3. Creating, protecting, and retaining Covered Information System audit records, reports, and supporting documentation to enable reviewing, monitoring, analysis, investigation, reconstruction, and reporting of unlawful, unauthorized, or inappropriate activity related to such Covered Information Systems and/or DOJ Information;
 4. Maintaining authorizations to operate any Covered Information System;
 5. Performing continuous monitoring on all such Covered Information Systems;
 6. Establishing and maintaining baseline configurations and inventories of Covered Information Systems, including hardware, software, firmware, and documentation, throughout the Information System Development Lifecycle, and establishing and enforcing security configuration settings for IT products employed in Information Systems;
 7. Ensuring appropriate contingency planning has been performed, including DOJ Information and Covered Information System backups;
 8. Identifying Covered Information System users, processes acting on behalf of users, or devices, and authenticating and verifying the identities of such users, processes, or devices, using multifactor authentication or HSPD-12 compliant authentication methods where required;
 9. Establishing an operational incident handling capability for Covered Information Systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities, and tracking, documenting, and reporting incidents to appropriate officials and authorities within Contractor's organization and the DOJ;
 10. Performing periodic and timely maintenance on Covered Information Systems, and providing effective controls on tools, techniques, mechanisms, and personnel used to conduct such maintenance;

11. Reserved.
 12. Protecting Covered Information System media containing DOJ Information, including paper, digital and electronic media; limiting access to DOJ Information to authorized users; and sanitizing or destroying Covered Information System media containing DOJ Information before disposal, release or reuse of such media;
 13. Limiting physical access to Covered Information Systems, equipment, and physical facilities housing such Covered Information Systems to authorized U.S. citizens unless a waiver has been granted by the Contracting Officer (“CO”), and protecting the physical facilities and support infrastructure for such Information Systems;
 14. Screening individuals prior to authorizing access to Covered Information Systems to ensure compliance with DOJ Security standards;
 15. Assessing the risk to DOJ Information in Covered Information Systems periodically, including scanning for vulnerabilities and remediating such vulnerabilities in accordance with DOJ policy and ensuring the timely removal of assets no longer supported by the Contractor;
 16. Assessing the security controls of Covered Information Systems periodically to determine if the controls are effective in their application, developing and implementing plans of action designed to correct deficiencies and eliminate or reduce vulnerabilities in such Information Systems, and monitoring security controls on an ongoing basis to ensure the continued effectiveness of the controls;
 17. Monitoring, controlling, and protecting information transmitted or received by Covered Information Systems at the external boundaries and key internal boundaries of such Information Systems, and employing architectural designs, software development techniques, and systems engineering principles that promote effective security; and
 18. Identifying, reporting, and correcting Covered Information System security flaws in a timely manner, providing protection from malicious code at appropriate locations, monitoring security alerts and advisories and taking appropriate action in response.
- B. Contractor shall not process, store, or transmit DOJ Information using a Covered Information System without first obtaining an Authority to Operate (“ATO”) for each Covered Information System. The ATO shall be signed by the Authorizing Official for the DOJ component responsible for maintaining the security, confidentiality, integrity, and availability of the DOJ Information under this contract. The DOJ standards and requirements for obtaining an ATO may be found at DOJ Order 2640.2, as amended. (For Cloud computing systems, see below.)
- C. Contractor shall ensure that no Non-U.S. citizen accesses or assists in the development, operation, management, or maintenance of any DOJ Information System, unless a waiver has been granted by the DOJ Component Head (or his or her designee) responsible for the DOJ Information System, the DOJ Chief Information Officer, and the DOJ Security Officer.
- D. When requested by the DOH CO or COR, or other DOJ official as described below, in connection with DOJ’s efforts to ensure compliance with security requirements and to maintain and safeguard against threats and hazards to the security, confidentiality,

integrity, and availability of DOJ Information, Contractor shall provide DOJ including the Office of Inspector General (“OIG”) and Federal law enforcement Components, (1) access to any and all information and records, including electronic information, regarding a Covered Information Systems, and (2) physical access to Contractor’s facilities, installations, systems, operations, documents, records, and databases. Such access may include independent validation testing of controls, system penetration testing, and FISMA data reviews by DOJ or agents acting on behalf of DOJ, and such access shall be provided within 72 hours of the request. Additionally, Contractor shall cooperate with DOJ’s efforts to ensure, maintain, and safeguard the security, confidentiality, integrity, and availability of DOJ Information.

- E. The use of Contractor-owned laptops or other portable digital or electronic media to process or store DOJ Information covered by this clause is prohibited until Contractor provides a letter to the DOJ CO, and obtains the CO’s approval, certifying compliance with the following requirements:
 - 1. Media shall be encrypted using a NIST FIPS 140-2 approved product;
 - 2. Contractor must develop and implement a process to ensure that security and other applications software is kept up-to-date;
 - 3. Where applicable, media shall utilize antivirus software and a host-based firewall mechanism;
 - 4. Contractor must log all computer-readable data extracts from databases holding DOJ information and verify each extract including such data has been erased within 90 calendar days of extraction or that its use is still required. All DOJ Information is sensitive information unless specifically designated as non-sensitive by the Department; and,
 - 5. A Rules of Behavior (“ROB”) form must be signed by users. These rules must address at a minimum: authorized and official use; prohibition against unauthorized users and use, and the protection of DOJ Information. The form also must notify the user that he or she has no reasonable expectation of privacy regarding any communications transmitted through or data stored on Contractor-owned laptops or other portable digital or electronic media.
- F. Contractor-owned removable media containing DOJ Information shall not be removed from DOJ facilities without prior approval from the DOJ CO or COR.
- G. When no longer needed, all media must be processed (sanitized, degaussed, or destroyed) in accordance with DOJ security requirements.
- H. Contractor must keep an accurate inventory of digital or electronic media used on DOJ contracts.
- I. Contractor must remove all DOJ Information from Contractor media and return all such information to the DOJ within 15 calendar days of the expiration or termination of the contract, unless otherwise extended by the CO, or waived (in part or whole) by the CO, and all such information shall be returned to the DOJ in a format and form acceptable to the DOJ. The removal and return of all DOJ Information must be accomplished in accordance with DOJ IT Security Standard requirements, and an official of the Contractor shall provide a written certification certifying the removal and return of all

such information to the CO within 15 calendar days of removal and return of all DOJ Information.

- J. DOJ, at its discretion, may suspend Contractor's access to any DOJ Information or terminate the contract, when DOJ suspects that Contractor has failed to comply with any security requirement, or in the event of an Information System Security Incident (see below) where the Department determines that either event gives cause for such action. The suspension of access to DOJ Information may last until such time as DOJ, in its sole discretion, determines that the situation giving rise to such action has been corrected or no longer exists. Contractor understands that any suspension or termination in accordance with this provision shall be at no cost to the DOJ, and that upon request by the CO, Contractor must immediately return all DOJ information to DOJ, as well as any media upon which DOJ Information resides, at Contractor's expense.

Cloud Computing

- A. **Cloud Computing** means an Information System having the essential characteristics described in NIST SP 800-145, *The NIST Definition of Cloud Computing*. For the sake of this provision and clause, Cloud Computing includes Software as a Service, Platform as a Service, and Infrastructure as a Service, and deployment in a Private Cloud, Community Cloud, Public Cloud, or Hybrid Cloud.
- B. Contractor may not utilize the Cloud system of any CSP unless:
1. The Cloud system and CSP have been evaluated and approved by a Third Party Assessing Organization (3PAO) certified under FedRAMP and Contractor has provided the most current Security Assessment Report ("SAR") to the DOJ CO for consideration as part of Contractor's overall System Security Plan, and any subsequent SARs within 30 calendar days of issuance; and has received an ATO from the Authorizing Official for the DOJ component responsible for maintaining the security confidentiality, integrity, and availability of the DOJ Information under contract; or,
 2. If not certified under FedRAMP, the Cloud System and CSP have received and ATO signed by the Authorizing Official for the DOJ component responsible for maintaining the security, confidentiality, integrity, and availability of the DOJ Information under the contract.
- C. Contractor must ensure that the CSP allows DOJ to access and retrieve any DOJ Information processed, stored or transmitted in a Cloud system under this Contract within a reasonable time of any such request, but in no event less than 48 hours from the request. To ensure that the DOJ can fully and appropriately search and retrieve DOJ Information from the Cloud system, access shall include any schemas, meta-data, and other associated data artifacts.

Information System Security Breach or Incident

- A. Definitions
1. **Confirmed Security Breach** (hereinafter, "Confirmed Breach") means any confirmed unauthorized exposure, loss of control, compromise, exfiltration,

manipulation, disclosure, acquisition, or accessing of any Covered Information System or any retrievable from, processed by, stored on, or transmitted within, to or from any such system.

2. **Potential Security Breach** (hereinafter, "Potential Breach") means any suspected, but unconfirmed, Covered Information System Security Breach.
 3. **Security Incident** means any Confirmed or Potential Covered System Security Breach.
- B. **Confirmed Breach.** Contractor shall immediately (and in no event later than within 1 hour of discovery) report any Confirmed Breach to the DOJ CO and the CO's Representative ("COR"). If the Confirmed Breach occurs outside of regular business hours and/or neither the DOJ CO nor the COR can be reached, Contractor must call DOJCERT at 1-866-US4-CERT (1-866-874-2378) immediately (and in no event later than within 1 hour of discovery of the Confirmed Breach), and shall notify the CO and COR as soon as practicable.
- C. **Potential Breach.**
1. Contractor shall report any Potential Breach within 72 hours of detection to the DOJ CO and the COR, *unless* Contractor has (a) completed its investigation of the Potential Breach in accordance with its own internal policies and procedures for identification, investigation and mitigation of Security Incidents and (b) determined that there has been no Confirmed Breach.
 2. If Contractor has not made a determination within 72 hours of detection of the Potential Breach whether a Confirmed Breach has occurred, Contractor shall report the Potential Breach to the DOJ CO and COR within one-hour (i.e., 73-hours from detection of the Potential Breach). If the time by which to report the Potential Breach occurs outside of regular business hours and/or neither the DOJ CO nor the COR can be reached, Contractor must call the DOJ Computer Emergency Readiness Team (DOJ-CERT) at 1-866-US4-CERT (1-866-874-2378) within one-hour (i.e., 73 hours from detection of the Potential Breach) and contact the DOJ CO and COR as soon as practicable.
- D. Any report submitted in accordance with paragraphs (B) and (C), above, shall identify(1) both the Information Systems and DOJ Information involved or at risk, including the type, amount, and level of sensitivity of the DOJ Information and, if the DOJ Information contains PII, the estimated number of unique instances of PII, the estimated number of unique instances of PII, (2) all steps and processes being undertaken by Contractor to minimize, remedy, and/or investigate the Security Incident, (3) any and all other information as required by the US-CERT Federal Incident Notification Guidelines, including the functional impact, information impact, impact to recoverability, threat vector migration details, and all available incident details; and (4) any other information specifically requested by the DOJ. Contractor shall continue to provide a written updates to the DOJ CO regarding the status of the Security Incident at least every three (3) calendar days until informed otherwise by the DOJ CO.
- E. All determinations regarding whether and when to notify individuals and/or federal agencies potentially affected by a Security Incident will be made by DOJ senior officials or the DOJ Core Management Team at the DOJ's discretion.

- F. Upon notification of a Security Incident in accordance with this section, Contractor must provide to DOJ full access to any affected or potentially affected facility and/or Information System, including access by the DOJ OIG and Federal law enforcement organizations, and undertake any and all response actions DOJ determines is required to ensure the protection of DOJ Information, including providing all requested images, log files, and event information to facilitate rapid resolution of any Security Incident.
- G. DOJ, at its sole discretion, may obtain, and Contractor shall permit, the assistance of other federal agencies and/or third party contractors or firms to aid in response activities related to any Security Incident. Additionally, DOJ, at its sole discretion, may require Contractor to retain, at Contractor's expense, a Third Party Assessing Organization (3PAO), acceptable to DOJ, with expertise in incident response, compromise assessment, and federal security control requirements, to conduct a thorough vulnerability and security assessment of all affected Information Systems.
- H. Response activities related to any Security Incident undertaken by DOJ, including activities undertaken by Contractor, other federal agencies, and any third-party contractors or firms at the request or direction of DOJ, may include inspections, investigations, forensic reviews, data analyses and processing, and final determinations of responsibility for the Incident and/or liability for any additional response activities. Contractor shall be responsible for all costs and related resource allocations required for all such response activities related to any Security Incident, including the cost of any penetration testing.

Personally Identifiable Information Notification Requirement

By signing this task order, the Contractor certifies that it has a security policy in place that contains procedures to promptly notify any individual whose Personally Identifiable Information ("PII") was, or is reasonably determined by DOJ to have been, compromised. Any notification shall be coordinated with the DOJ CO and shall not proceed until the DOJ has made a determination that notification would not impede a law enforcement investigation or jeopardize national security. The method and content of any notification by Contractor shall be coordinated with, and subject to the approval of DOJ. Contractor shall be responsible for taking corrective action consistent with the DOJ Data Breach Notification Procedures and as directed by the DOJ CO, including all costs and expenses associated with such corrective action, which may include providing credit monitoring to any individuals whose PII was actually or potentially compromised.

Pass-through of Security Requirements to Subcontractors and CSPs

The requirements set forth in the preceding paragraphs of this clause apply to all subcontractors and CSPs who perform work in connection with this Contract, including any CSP providing services for any other CSP under this Contract, and Contractor shall flow down this clause to all subcontractors and CSPs performing under this contract. Any breach by any subcontractor or CSP of any of the provisions set forth in this clause will be attributed to Contractor.

H.6 Standards of Conduct

(a) In performing this contract, Contractor personnel may be required to interact with government and non-government officials at various levels. The Contractor shall ensure that all its personnel assigned to this contract conduct their work in a courteous, professional and responsible manner, both in appearance and in deed. The standards of conduct for DOJ and/or other client agency employees at the facility(ies) where the task services are rendered shall apply to all ITSS-5 Contractor personnel working on or at the same DOJ owned or leased work space(s).

(b) Guidelines for the Contractor to screen its proposed employees for suitability and conduct are contained in Attachment 3 of this contract – but these are not a substitute for other standards of conduct which may also apply at the facilities where services will be rendered.

H.7 Contractor Responsibility for Assigned Space and Equipment

(a) The Contractor shall be responsible for maintaining all assigned work space(s) in a clean and orderly fashion during the period of this contract. Furniture as may be assigned to the space(s) shall remain in place and not be removed from these areas.

(b) The Contractor shall be solely responsible for exercising control over any supplies, materials and equipment belonging to either its employees or the company which may be utilized on the Government's site.

H.8 Indemnification

(a) Responsibility for Government-owned or leased Property and Equipment. During performance, the Contractor shall be responsible for all negligent acts or omissions of its employees or agents or the employees or agents of its subcontractor(s). In this regard, the Contractor shall, at no cost to the Government and at the Government's option, replace or compensate the Government for any damage to or loss of Government-owned or -leased property caused by such negligent acts or omissions.

(b) Responsibility for Contractor or Third-party owned or leased Property and Equipment. The Contractor shall indemnify the Government against any and all liability claims for loss or damage to any Contractor owned or leased property occurring as a result of negligence or omissions by employees or agents of the Contractor or its subcontractor(s) in connection with the performance of work under the terms of this delivery order.

(c) Responsibility for Property and Equipment Damaged or Lost through no fault of the Contractor or the Government. Property damage or loss that occurs through no fault of either the Contractor, their subcontractors or agents or the Government shall be the responsibility of the party holding title to or having leased the property.

(d) Contractor Actions. The Contractor shall indemnify and hold the Government, its agents and employees, harmless against any financial loss or liability, including costs and expenses, arising from any negligent or wrongful act, or omission, or malpractice, on the part of the Contractor, or any of its agents or employees, during the Contractor's performance under this delivery order. The Contractor also agrees that if the Government suffers any financial loss

or liability because of any negligent or wrongful act, or omission, or malpractice, by the Contractor, or any of its agents or employees, the Department may offset any such sums against any money in the Department's possession, which would otherwise be due and payable to the Contractor.

H.9 Publicity

Press releases or other publicity such as website announcements made in connection with this contract shall not be made by the Contractor, unless and until prior written consent has been provided from the Contracting Officer. The ITSS-5 Contractor shall submit its draft press release(s) to the Procuring Contracting Officer (PCO), who shall coordinate the language with the DOJ Office of the Chief Information Officer (CIO), and the DOJ Office of Public Affairs (OPA), prior to giving final authorization. This process has been known to take anywhere from fifteen to thirty (15-30) days to complete from receipt of a draft press release and the ITSS-5 Contractor acknowledges this fact when signing the contract.

(a) In order to provide equity of processing press releases or other award announcements, all ITSS-5 Contractors shall submit their drafts within two business days after award of the ITSS-5 contract(s) to the PCO. The PCO shall batch process and coordinate all the press releases to the appropriate offices specified above, and issue his/her written consent(s) at the same time to all ITSS-5 Contractors. If one or a low number of the press releases is/are holding up consent for the many, then the PCO reserves the right to provide consent to the many and continue processing the other press releases.

(b) Nothing in this provision prohibits DOJ from making Agency award announcements or congressional notifications it deems appropriate.

H.10 Freedom of Information Act Requests for Contractor's Proposal

With respect to a Freedom of Information Act (FOIA) request for any part of the Contractor's technical proposal that is either set forth or incorporated by reference in this contract, before responding to the FOIA request the Department will afford the Contractor an opportunity to explain why it believes some or all of the relevant parts of the technical proposal may be exempt from release under the FOIA.

H.11 Subcontracts and Administrative Contracting Officer (ACO) Consent

(a) Subcontracting is not restricted under this contract if it does not adversely affect the quality or delivery of the final product or service. The ACO shall have the right to restrict subcontracting if it is determined that such an action is in the best interest of the Government.

(b) Subcontractors named and described in the Contractor's successful proposal are considered authorized to perform work under this contract without further written consent from the ACO, unless such consent is revoked by the ACO. Other proposed subcontractors must be

identified in task proposals and written consent must be provided by the ACO, prior to starting the work.

H.12 Prohibition Against Soliciting and Performing Personal Services

(a) The performance of personal services under this contract is strictly prohibited.

(b) Personal service contracting is described in Section 37.104 of the Federal Acquisition Regulations (FAR). There are a number of factors, when taken individually or collectively, which may constitute personal services. Each contract arrangement must be judged in light of its own facts and circumstances, but the question relative to personal services is: Will the Government exercise relatively continuous supervision and control over the contractor personnel performing this contract?

(c) The government and the Contractor understand and agree that the support services to be delivered under this contract are non-personal services in nature. That is no employer-employee relationships exist or will exist under the contract between the government and the contractor or between the Government and the contractor's employees.

(d) Contractor personnel under this contract shall not:

1. Be placed in a position where they are appointed or employed by a Federal employee, or are under the supervision, direction, or evaluation of a Federal employee.
2. Be placed in a Federal staff or policy making position.
3. Be placed in a position of supervision, direction, or evaluation over DOJ personnel, or personnel of other contractors, or become a part of a government organization.

(e) Employee Relationship

1. The services to be performed under this contract do not require the contractor or its employees to exercise personal judgment and discretion on behalf of the government.
2. Rules, regulations, direction, and requirements which are issued by DOJ management under their responsibility for good order, administration, and security are applicable to all personnel who enter a Government installation. This is not to be construed or interpreted to establish any degree of Government control which is inconsistent with a non-personal services contract.
3. The Contractor shall immediately advise the Contracting Officer if the contractor or its employees are directed by any Government employee to perform work that the Contractor believes constitutes personal services.

(f) Contractor Management Responsibility

The Contractor shall appoint a supervisor/manager who will be the contractor's authorized representative for technical and administrative performance of all services required hereunder. The supervisor shall provide the single point of contact through which all contractor/government communications, work, and technical direction shall flow. The supervisor shall receive and execute, on behalf of the Contractor, such technical direction as the COTR may issue within the terms and conditions of the contract. All administrative support of contractor technical personnel required to fulfill the tasks assigned under this contract shall be the responsibility of the contractor.

H.13 Insurance

In accordance with clause 52.228-5 "Insurance - Work on a Government Installation" (see Section I.1) and this schedule, the Contractor shall acquire and maintain during the entire performance period of this contract insurance of at least the following kinds and minimum amounts set forth below:

- (1) Workman's Compensation and Employers' Liability Insurance in accordance with the amounts specified by the laws of the states in which the work is to be performed under this contract. In the absence of such state laws, an amount of \$100,000 shall be required and maintained.
- (2) General Liability Insurance - Bodily injury liability in the minimum amount of \$500,000 per occurrence.
- (3) Automobile Liability Insurance in the amount of \$200,000 per person and \$500,000 per occurrence for bodily injury, and \$20,000 per occurrence for property damage.

H.14 Type of Contract (APR 1984) FAR 52.216-1

This is a fixed unit price, indefinite delivery, indefinite quantity task order type contract. Individual task orders placed under the proposed contracts may be issued on a labor-hour, time-and-materials, or firm fixed-price basis.

H.15 Small Business Subcontracting Plan Requirements

(a) The Contractor's contract specific or approved corporate-wide plan shall provide for a fair portion of the work awarded to be subcontracted to Small, Veteran-Owned Small, Disabled Veteran-Owned Small, HUB Zone Small, Small Disadvantaged, and Women-Owned Small Businesses. Due to the uncertainty of exactly what work a given ITSS-5 contractor will capture after contract award, and in accordance with DOJ policy on this matter, there are no specific minimum mandated goals for small business subcontracting under this contract. The government-wide total goal is 40% of the *total planned subcontracting dollars*. The Offeror must set-forth in its proposal for this ITSS-5 contract what it believes are the fair and proper goals for each of the various types of small businesses listed in Attachment 5. The Government's suggested goals, based on statutory minimum levels, are as follows:

Business Size	Suggested Percentage Goal
Small Business	40%
Small Disadvantaged Small Business	5%
Woman-Owned Small Business	5%
HUBZone Business	3%
Veteran-Owned Small Business	3%
Service-Disabled Veteran Owned Small Business	3%

(b) The *total planned subcontracting dollars* can and will vary from contractor to contractor, depending on the Contractor's make or buy decisions made to obtain an ITSS-5 contract, and further to capture specific task work. The Contractors' proposed plan shall indicate the annual and total amount of planned subcontract dollars and percentages of *planned subcontracting dollars* for all subcontracted business types, large or small.

(c) The Small Business Subcontracting Plan submitted by _____ dated _____, as definitized in Section H.24 concerning the delivery of reports, has been approved by the Contracting Officer and is incorporated herein and made a part of this contract as Section J, Attachment 5.

Note: Section H.15 requirements apply only to the Unrestricted Track. It does not apply to Small Businesses as defined under this solicitation/contract.

H.16 Facility Access

(a) Rights of Egress and Ingress

During the life of this contract, the rights of ingress to and egress from the Department of Justice facility for the Contractor's representatives shall be made available as required. During all operations on Government premises, the Contractor's personnel shall comply with the rules and regulations governing the conduct of personnel and the operation of the facility. The Government reserves the right to require Contractor personnel to "sign-in" upon entry and "sign-out" upon departure from the Department of Justice facility.

(b) Building Access Passes

1. When any Contractor or subcontractor personnel enter a DOJ building for the first time, the Contractor shall allow one hour for security processing and the fabrication of buildings access passes.
2. Passes shall be subject to periodic review by the Contractor's Supervisor and checked against the employee's personal identification. The Contractor's employees shall present themselves for the issuance of renewed passes when required by the Government as scheduled by the COTR or his designee. The Contractor shall notify the COTR when employee passes are lost, and must immediately apply for reissuance of a replacement pass. It is the Contractor's

responsibility to return passes to the COTR or his designee when a Contractor employee is dismissed, terminated or assigned to duties not within the scope of this contract.

H.17 Personnel Requirements (Hiring)

The Contractor shall not hire any employee with the specific purpose of providing interim employment for the employee until employment by the Government can be effected.

H.18 Confidentiality of Data

(a) Duplication or disclosure of the data and other information to which the Contractor will have access as a result of this contract is prohibited. The terms "Contractor" and "contract employee" in this clause include all entities and individuals that will perform under this contract, including the Contractor, team member, subcontractor, consultant, and/or independent contractor. It is understood that throughout performance of this contract, the Contractor will have access to confidential data which is either the sole property of the Department of Justice or is the sole property of other than the contracting parties. The Contractor agrees to maintain the confidentiality of all data to which access may be gained throughout contract performance, whether title thereto vests in the Department of Justice or otherwise. "Data" in this context also includes any information about the cases or investigations the contractor is working on, including the names and subject matters of the cases or investigations. The Contractor agrees not to disclose or divulge any such information except to persons who:

Have a DOJ security approval,
Have signed the DOJ Non-Disclosure Agreement, and
Have a need to know.

This limitation specifically applies to the Contractor's management chain.

(b) The Contractor agrees to not disclose said data, any interpretations and/or translations thereof, or data derivative therefrom, to unauthorized parties in contravention of these provisions, without the prior written approval of the Contracting Officer or the party in which title thereto is wholly vested. The Contractor may be held responsible for any violations of confidentiality.

(c) The Contractor agrees that upon termination of the contract, it has no property or possessory right to any of the correspondence, files or materials, of whatever kind and description, or any copies or duplicates of such, whether developed/prepared by the Contractor or furnished by the Government in connection with the performance of this contract; and that, upon demand, the Contractor will surrender immediately to the COTR such items, matters, materials, and copies.

(d) All contract employees who will have access to confidential data will be asked to sign a Confidentiality Agreement (Attachment 3). It is the responsibility of the Contractor to assure that such Agreements have been signed before access to confidential data is permitted.

H.19 Government Rights in Data and Computer Software

(a) The Government shall have unlimited rights, as delineated in FAR Clause 52.227-14, which is incorporated by reference in Section I herein, in all computer software, documentation, and other data developed by the Contractor under this contract.

(b) The Contractor shall not duplicate or disclose in any manner, for any purpose whatsoever, or have or permit others to do so, any of the computer software, documentation, and other data developed by the Contractor under this contract.

(c) The Government shall have restricted rights, as delineated in Alternate III of the FAR clause 52.227-14, in all restricted computer software furnished by the Contractor under this contract.

H.20 Proprietary Rights**(a) Government Furnished Data and Materials**

The DOJ shall retain all rights and privileges, including those of patent and copy, to all Government furnished data. The Contractor shall neither retain nor reproduce for private or commercial use any data or other materials furnished under this contract. The Contractor agrees not to assert any rights at common law or in equity or establish any claim to statutory copyright in such data. These rights are not exclusive and are in addition to any other rights and remedies to which the Government is otherwise entitled elsewhere in this contract.

(b) Contractor Produced Data and Materials

All property rights, including publication rights, in the information and materials produced by the Contractor in connection with this contract shall vest in the Government. Information and materials shall include: progress reports, computer software applications/data bases, software documentation, plans, systems analyses, reports, extracts, test data and procedures.

H.21 Section 508 Compliance

By authorized signature on this contract, the contractor certifies that it shall comply with Section 508 of the Rehabilitation Act of 1973 where and when applicable, or when it has otherwise been determined by the Administrative Contracting Officer (for future acquisitions) that the Section 508 rules/guidance are applicable to individual Electronic and Information Technology (EIT) product or EIT service acquisitions made on behalf of DOJ under this ITSS-5 contract.

H.22 Electronic Subcontracting Reporting System (eSRS) – Interim Procedures

This solicitation and/or contract incorporates by reference, in Section I, FAR clause 52.219-9. Paragraph (j) of this clause requires contractors submit Standard Forms (SFs) 294 and 295 and ensure that its subcontractors agree to submit SFs 294 and 295.

The Electronic Subcontracting Reporting System (eSRS) is accessible on the internet at www.esrs.gov.

H.23 Clauses Incorporated by Reference

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this address: <http://www.acquisition.gov/far/>

CLAUSE NO.	DATE	TITLE
52.216-22	Oct 1995	Indefinite Quantity - paragraph (d) insert "183 days from the last task order issued under the Option to Extend Services provision at F.1.2".

H.24 Off-Ramp

Each ITSS-5 Contractor is expected to participate in the ordering process by submitting proposals in response to Work Plan Requests (WPRs) for which the Contractor has a reasonable chance for award, to successfully perform the terms of their task orders, and to promptly improve performance when it does not meet the terms of the task orders. If an ITSS-5 Contractor does not meet these expectations, it is the Government's intent to "off-ramp" the Contractor by allowing the Base Period to expire and not exercising Option Period one. In addition, at the end of the Base Period the Government will "off-ramp" those Small Business Track Contractors that no longer meet the size standards identified in SOW section A.3.

ITSS-5 contract holders under the Small Business Track will be required to re-represent their size status prior to exercise of the option period. Prime Contractors in the Small Business Track that are no longer small may be moved to the Unrestricted Track.

H.25 On-Ramp

The Government reserves the right to utilize an "On Ramp" concept to manage the recertification process and maintain a sufficient number of contract awardees for the ITSS-5 Small Business Track.

The Government has determined the need that at all times during the term of the ITSS-5 contracts there remain an adequate number of Small Business Prime contractors eligible to compete for TOs. The Government intends to periodically review the total number of ITSS-5 Small Business Prime contractors participating in the ordering process, and determine whether it would be in the Government's best interest to initiate an open season to add new contractors to the ITSS-5 contract program. This is a discretionary, unilateral authority of the Government,

and may be used in any of the small business set-aside categories. In addition, it is anticipated that one or more Small Business Track Prime contractors will no longer qualify under Small Business size standards at the expiration of the Base Period.

The Government also reserves the right to utilize an "On Ramp" concept for the ITSS-5 Unrestricted Business Track at any time during the term of the contract.

H.26 Open Season Procedures

If DOJ determines that it would be in the Government's best interest to open a new solicitation to add new contractors to the ITSS-5 Small Business and/or Unrestricted Track(s), the CO may do so at any time provided that:

- (a) The open season solicitation is issued under then-applicable Federal procurement law;
- (b) The open season solicitation identifies the total approximate number of new awards that the ITSS-5 CO intends to make. The CO may decide to award more or fewer ITSS-5 contracts than the number anticipated in the solicitation depending upon the overall quality of the offers received;
- (c) The award decision under any open season solicitation is based upon substantially the same evaluation factors/sub-factors as the original ITSS-5 solicitation;
- (d) The terms and conditions of any resulting awards from an open season solicitation are materially identical to the existing version of the basic ITSS-5 contracts;
- (e) The term for any such new awards from an open season solicitation is co-terminus with the existing term for all other ITSS-5 Small Business and/or Unrestricted Track contracts, including the option period;
- (f) If awarded an ITSS-5 contract through the open season authority, any new ITSS-5 Small Business or Unrestricted Prime contractor is eligible to compete for task orders with the same rights and obligations as any other ITSS-5 Small Business and/or Unrestricted Track contractor; and
- (g) The award of any new ITSS-5 contract(s) does not increase the overall ceiling of the ITSS-5 contract program.

H.27 Acquisitions and Mergers

If the size of a Small Business Prime contractor changes due to an acquisition or merger at any point during the life of the contract, the Prime contractor must notify the ITSS-5 CO within thirty (30) days. If it is deemed that the contractor is no longer a small business, they can no longer participate in any future task order competitions under the ITSS-5 program, but will be able to complete the work on current task orders. Once the current task order(s) are complete, the contractor will be removed from the ITSS-5 contract.

H.28 Continuing Contract Performance during a Pandemic Influenza or other National Emergency

(a) During a Pandemic or other emergency we understand that our contractor workforce will experience the same high levels of absenteeism as our federal employees. Although the

Excusable Delays and Termination for Default clauses used in government contracts list epidemics and quarantine restrictions among the reasons to excuse delays in contract performance, we expect our contractors to make a reasonable effort to keep performance at an acceptable level during emergency periods.

(b) The Office of Personnel Management (OPM) has provided guidance to federal managers and employees on the kinds of actions to be taken to ensure the continuity of operations during emergency periods. This guidance is also applicable to our contract workforce. Contractors are expected to have reasonable policies in place for continuing work performance, particularly those performing mission critical services, during a pandemic influenza or other emergency situation.

(c) The types of actions a federal contractor should reasonably take to help ensure performance are:

- Encourage employees to get inoculations or follow other preventive measures as advised by the public health service.
- Contractors should cross-train workers as backup for all positions performing critical services. This is particularly important for work such as guard services where telework is not an option.
- Implement telework to the greatest extent possible in the workgroup so systems are in place to support successful remote work in an emergency.
- Communicate expectations to all employees regarding their roles and responsibilities in relation to remote work in the event of a pandemic health crisis or other emergency.
- Establish communication processes to notify employees of activation of this plan.
- Integrate pandemic health crisis response expectations into telework agreements.
- With the employee, assess requirements for working at home (supplies and equipment needed for an extended telework period). Security concerns should be considered in making equipment choices; agencies or contractors may wish to avoid use of employees' personal computers and provide them with PCs or laptops as appropriate.
- Determine how all employees who may telework will communicate with one another and with management to accomplish work.
- Practice telework regularly to ensure effectiveness.
- Make it clear that in emergency situations, employees must perform all duties assigned by management, even if they are outside usual or customary duties.
- Identify how time and attendance will be maintained.

(d) It is the contractor's responsibility to advise the government contracting officer if they anticipate not being able to perform and to work with the Department to fill gaps as necessary. This means direct communication with the contracting officer or, in his/her absence, another responsible person in the contracting office via telephone or email messages acknowledging the contractor's notification. The incumbent contractor is responsible for assisting the Department in estimating the adverse impacts of nonperformance and to work diligently with the Department to develop a strategy for maintaining the continuity of operations.

(e) The Department does reserve the right in such emergency situations to use federal employees, employees of other agencies, contract support from other existing contractors, or to enter into new contracts for critical support services. Any new contracting efforts would be acquired following the guidance in the Office of Federal Procurement Policy issuance "Emergency Acquisitions", May 2007 and Subpart 18.2, Emergency Acquisition Flexibilities, of the Federal Acquisition Regulations.

NOTE: Sections I, J, K, L, and M are not included for Industry Comment