Description of document:	Department of Justice (DOJ), Justice Management Division (JMD) contractual documents for the procurement of an automated FOIA tracking/processing system for the Department of Justice, 2007-2012
Requested date:	02-October-2011
Released date:	08-August-2012
Posted date:	04-March-2013
Source of document:	FOIA Contact Justice Management Division Department of Justice Room 1111 RFK, 950 Pennsylvania Avenue, NW Washington, DC 20530-0001 Fax: 202-616-6695 Email: JMDFOIA@usdoj.gov

U.S. Department of Justice

Justice Management Division

Office of General Counsel

Washington, D.C. 20530

AUG 0 8 2012

RE: Request for documents related to Contract DJJ-09-F-1791 (JMD FOIA Tracking Number 2429133)

I am responding on behalf of the Justice Management Division (JMD) to your Freedom of Information Act (FOIA) request dated October 2, 2011, which asked for the Statement of Work for this contract, a copy of the successful bidder's technical proposal, and a copy of the reports submitted in the furtherance of this contract.

We have searched the records of the JMD Procurement Services Staff (PSS) for documents responsive to your request. Your request is granted in part and denied in part. Some information within the scope of your request is exempt from disclosure under Exemption 3 of the FOIA, which prohibits disclosure of matters specifically exempted from disclosure by statute. Pursuant to 41 U.S.C. § 4702 (formerly 41 U.S.C. § 253b(m)) an executive agency may not release a proposal under the FOIA unless the proposal has been set forth or incorporated by reference in a contract entered into between the agency and the contractor that submitted the proposal. The technical proposal, including Attachment E (the completed Requirements Matrix) was not incorporated into the final contract. Accordingly, we are withholding it under Exemption 3. With respect to submitted reports in furtherance of this contract, there are no reports in the PSS official contract file. We are providing you with the Statement of Work and a blank copy of the Requirements Matrix for this contract at no cost to you.

If you are dissatisfied with my action, Department regulations at 28 C.F.R. § 16.9 provide that you may file an appeal within 60 days of the date of this letter by writing to the Office of Information Policy, U.S. Department of Justice, 1425 New York Avenue, Suite 11050, Washington , D.C. 20530. Both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal."

Sincerely,

Arthur E. Gary
General Counsel

Enclosures

The BPA Ordering Periods are as follows:

Table 1 - BPA Ordering Periods	
Base Year	February 27, 2009 through February 26, 2010
Order Period #1	February 27, 2010 through February 26, 2011
Order Period #2	February 27, 2011 through February 26, 2012
Order Period #3	February 27, 2012 through February 26, 2013
Order Peirod #4	February 27, 2013 through February 26, 2014

BPA Calls to be issued under the proposed BPA will be issued on a firm fixed price, labor hour, or time-and-materials basis. The unit prices in the Pricing Table shall be fixed unless a price reduction(s) is effected via formal modification by mutual agreement between the Contractor and the Contracting Officer. Additional CLINS may be added to the Pricing Table after award of the BPA by mutual agreement of the parties. Prices for additional CLINS shall reflect a discount at least equal to that offered for the CLINS included in the BPA at time of award. All orders placed against this BPA are subject to the terms and conditions of the GSA Schedule contract and this BPA.

2. Statement of Work

2.1 Background

The Department as a whole still lacks a complete automated system to handle FOIA requests. Most components are using inefficient, antiquated systems with no uniformity that handle the process only partially. A major part of the process is manually handled which is very costly and labor-intensive. In Fiscal Year (FY) 2007, the Department spent approximately $40 million dollars on processing FOIA requests.

In general, many components have basic case management and tracking systems that are at leastten years old. Other smaller components often have no systems, but may use spreadsheets to track requests and prepare their annual report. The Office of Information and Privacy (OIP) has taken the lead on the FOIA Automation System initiative. OIP is interested in securing an automated tracking and processing system and is prepared to run a pilot for the selected commercial off-the-shelf/government off-the-shelf (COTS/GOTS) product as a proof of concept. If it is determined that the Proof of Concept is a success in terms of meeting the Department's objectives, it is anticipated that the system will be considered for rollout to additional components.

2.2 Objectives

The primary objectives of this BPA are: 1) To implement an automated FOIA electronic tracking and processing system that significantly improves the tracking, processing, and reporting capabilities of the DOJ's FOIA requests and appeals process, while complying with applicable executive orders and statutory amendments; and 2) The system shall initially be implemented within OIP, and upon a successful implementation and usage period, the system may be implemented by additional components throughout the Department. The FOIA system shall:

1. Improve case tracking capabilities: type, status, fees, time spent on and disposition of cases
2. Provide for workflow management
3. Provide electronic searching and redaction of documents
4. Provide for system administration capabilities
5. Provide extensive reporting capabilities

6. Facilitate the creation of an annual report
7. Assist in sorting and organizing documents and the preparation of indices of documents
8. Increase processing speed and accuracy
9. Increase productivity
10. Increase quality controls

2.3 Project Assumptions

(a) The Department must comply with the FOIA, as amended by the Open Government Act of 2007 and OIP's written guidance related to the Act, to include the January 9, 2008, "Congress Passes Amendments to the FOIA" article and the "2008 Guidelines for Agency Preparation of Annual FOIA Reports." Executive Order 13,392: Improving Agency Disclosure of Information, which, among other requirements asks agencies to examine the use of information technology in responding to FOIA requests. According to the Executive Order, agencies must examine the use of information technology in responding to FOIA requests, including the tracking of FOIA requests and communication with requesters; practices with respect to requests for expedited processing; and identify ways to eliminate or reduce its FOIA backlog.The Department has government wide responsibility to issue instructions and guidance as appropriate to implement theFOIA and the FOIA Executive Order.

(b) The Department has a decentralized system for handlingFOIA requests. There are forty components with approximately three hundred (300) usersthat manually process, determine status of requests, and calculate fees for each FOIA request. In Fiscal Year 2007, DOJ spent approximately $40 million dollars processing FOIA requests.

(c) All FOIA report elements are the same (by law); therefore, allDOJ components and other federal agencies report on the same elements and in the same way. TheDepartment, like all federal agencies, is required to compile an annual report in accordance with 5 U.S.C. § 552(e)(1). Because the Department has a decentralized process for administering the FOIA, each component within Justice submits a report to OIP, which then compiles the Department's report. OIPprepares eight separate reports, one for each of the components for which it processes FOIA requests. In addition, OIP compiles a report concerning all administrative appeals of FOIA requests throughout the Department.

(d) The selected platform and architecture shall accommodate up to 300 users.

(e) Operating Environment -- The FOIA system should be an interactive system with online transactions and should allow for ad-hoc reporting. It should have a centralized database (Oracle or SQL Server) and about 40 local users interacting with the database for the Initial implementation phase. The number of additional users in the second phase will be determined on an on-going basis, as additional components implement the FOIA system.

(f) Processing – the FOIA system shall have the following processing functions for FOIA requests.

- **Initial Requests** – the process of receiving a FOIA request, logging it into the system, processing it (searching, reviewing and redacting the documents, conducting necessary consultations and referrals, and preparing a response), sending a response to the requester, tracking all processing functions, and closing the request. During this process, fees may be calculated and collected. Sorting and indexing of documents may be required.

- **Appeals** – the process of receiving an appeal, logging it into the system, reviewing the appeal and action taken on the initial request, including potential supplemental processing and release by OIP, drafting an appeal response, and sending the response.

- **DRC** – the process of receiving a mandatory declassification appeal or a FOIA appeal involving classified records, logging it into the system, preparing the case for DRC, preparing and sending a final response.

(g) Security - The FOIA system should adhere to the DOJ's C & A security requirements. Additionally, the system should support role-based security. The system should support assigning users to roles internal to the organization such as:

- Security Officer
- System Administrator
- Application Administrator
- Help Desk
- Users

(h) Development Environment - The Contractor can elect to perform development work at the DOJ Systems Development Services (SDS) facilities subject to proper notification, security clearance processing and approval of SEPS. The Contractor will have available a development environment at its own facility in which the Contractor can build and configure the application in order to expedite development and unit testing of the application. Fees or charges for the upkeep or potential enhancement of Contractor's facilities associated with this effort is not billable. The development environment can exist either within the DOJ SDS environment or at the Contractor's facility, or at both facilities. The Contractor shall specify its intention to use the DOJ environment or its own facilities in its proposal.

(i) Test Environment --The Contractor shall maintain a test environment capable of supporting unit testing and the integration testing of various system modules in the event that the Contractor elects to perform some or all development activities at the Contractor's facilities. Again, fees or charges associated with the use of Contractor's facilities for these services are not separately billable. For the purposes of system testing, DOJ integration testing, C & A testing and user acceptance testing, the application must be tested in DOJ's SDS facilities with the support and assistance of SDS personnel. As such, any changes to code and/or system configuration needed to ensure proper system operations in the DOJ environment must be tracked and managed according to the change control methods and procedures available within the SDS environment.

(j) Production Environment -- All FOIA system users shall be able to access the system using their existing computing and communications equipment and communications capabilities. The DOJ is responsible for the users' desktops and communication capabilities. The targeted production environment for the new FOIA system will be provided by the SDS organization based on design and specifications provided by the vendor for the initial implementation deployment. The environment will include: hardware and operating systems software needed to support the FOIA system, 24x7 systems availability, regular back up services, automatic failover and disaster recovery services. The production environment will be located at the Justice Data Center (JDC) located in Rockville, MD. The standby server (automatic failover) will also be located at the JDC. During the design of the system and throughout testing and implementation activities, the Contractor shall work closely with the SDS organization to ensure that the system works reliably and efficiently in the SDS environment and that the joint efforts of the Contractor and the SDS organization ensure the reliability, security and availability of the FOIA system to its users.

(k) At present, the following responsibilities apply to the successful operation and maintenance of the FOIA production and test environments:

The Contractor is responsible for:

- The development of user and systems administration procedures related to the successful configuration and management of the application software in the SDS operating environment.
- All application software and application software specific database maintenance, including patches, enhancements, upgrades and fixes.
- The development of software maintenance plans, configuration management plans and implementation plans throughout the course of the development and testing project tasks.
- Full planning, documentation and testing of system configuration and recovery/restart procedures.
- Technical training/knowledge transfer associated with properly training SDS and OIP's technical support personnel. Training and knowledge transfer should start early on in the project and continue throughout the project as the system is developed and implemented.
- Providing/ensuring support for application Help Desk operations (anticipating Tier 3 support level). See Attachment B, Help Desk Escalation Workflow.
- Regular performance monitoring and reporting including reviews of security audit logs.
- Application hosting recommendations, design based on requirements and project usage and data volumes.

SDS (working independently or through its relationship with OSS) is responsible for:

- All operating system patches, security fixes, and upgrades;
- All hardware and server maintenance and monitoring;
- Back up and recovery services associated with recovery of the processing environment and application;
- Systems administration of hardware, database and operating system environment;
- Providing Help Desk services (Tier 2);
- Working with the contractor in performance monitoring and performance resolution.

For more details regarding the operating environment see Attachment C: SDS Development Environment Infrastructure and Attachment D: Production Hosting High Level Design.

2.4 Scope

The scope of this BPA covers the planning, integration and implementation services that the Government may require in BPA Calls that may be issued under this BPA. Specific task requirements will be detailed in individual BPA Calls. The Department envisions that BPA Calls resulting from this BPA will be structured to allow significant flexibility for ordering and use. The Contractor shall provide the comprehensive FOIA electronic tracking and processing system that supports the Department's mission, vision, goals, and objectives to improve the tracking, processing, and reporting capabilities of all FOIA business processes.

BPA Calls for these services will include the requirements delineated in Sections 2.15, "Implementation Tasks and Deliverables". The specific requirements, deliverables, and desired schedule will be identified in a BPA Call proposal request that will be provided to the Contractor. The Contractor's task proposal must identify the approach, level of effort, staffing, and the total estimated cost to complete all of the requirements. The BPA Call proposal request process is designed to allow for the refinement of the bid submitted during the BPA solicitation period.

2.5 System Requirements

2.5.1 General Requirements

The Department desires that the FOIA system be implemented using industry-standard, easily supportable and highly expandable technology components. The target production processing environment for the FOIA system will be a Windows Server or AIX-based processing environment located at the Rockville Data Center and managed by the Systems Development Services (SDS) organization. This facility is capable of supporting development, testing and production processing environments associated with the FOIA System. At a minimum, the Contractor will install the new system in the targeted SDS environment to support integration testing, system certification and user acceptance testing requirements of the project.

The FOIA system must be an established COTS product.

In addition to the technical and functional system requirements specified in Attachment E "FOIA of Requirements Matrix", the system shall adhere to the following General System Requirements. Several government and DOJ-wide technical constraints and guidelines that must be observed are also included.

Table 2 - General System Requirements		
Function	**Ref**	**DOJ Requirement**
General	G1	The system shall be developed using either the J2EE or .Net framework architectures.
General	G2	The system shall support Oracle and/or SQL Server as the application's Relational Database Management System.
General	G3	If the system is a web-based application, the system shall be operational on DOJ versions of Netscape 4.7 or greater and DOJ versions of Microsoft IE 5.5 or greater.
General	G4	The system shall support the capability to export data in XML format.
General	G5	The system shall support the capability to import data from XML format.
General	G6	All data within the system or exchanged between systems should be treated at the level of sensitive but unclassified (SBU) However, the system should have the capability to treat classified data, if required.
General	G7	All users logging into the system must be unique, authenticated prior to enabling access, and comply with DOJ password management policies.
General	G8	Prior to final acceptance, the system shall be fully Certified and Accredited (C&A) by an independent source with no technical findings.
General	G9	The system shall have the ability to interface with industry standard Enterprise Documents Management Systems

In addition to the above general system-specific requirements and the more detailed requirements to follow, the Contractor shall understand and adhere to the overall government and DOJ standards noted below in Sections 2.5.2. and 2.5.3. These overall standards are available for reference via government web sites and are not included in this document.

2.5.2 General Federally Mandated Constraints

- Federal Information Security Management Act (FISMA)
- Government Performance and Results Act (GPRA)
- Paperwork Reduction Act (PRA)
- Government Paperwork Elimination Act (GPEA)
- Clinger-Cohen Act (CCA)
- Section 508 of the Workforce Investment Act of 1998
- OMB Circular No. A-130 (including Appendix III) security constraints
- Public Law 93-579, The Privacy Act of 1974
- Public Law 99-474, Computer Fraud Act of 1986
- Presidential Decision Directive PDD-63
- Freedom of Information Act, 5 USC 552, and as amended, Privacy Act of 1974, 5 USC 552a
- Computer security Act of 1987 (Pub. Law 100-135)

2.5.3 Department of Justice Technical Constraints

- IT Strategic Plan (http://www.usdoj.gov/jmd/ocio/it-strategic-plan.htm)
- Enterprise Architecture Plan (Provided upon request)
- Technical Reference Model (Provided upon request)
- DOJ System Development Life Cycle (SDLC) (http://www.usdoj.gov/jmd/irm/lifecycle/table.htm)
- JCON II Standard Architecture and JCON-IIA Standards (Provided upon request)
- DOJ Orders for security: 2620.7, 2640.1, 2830.1D, 2640E (http://10.173.2.12/dojorders/dojorders.php)
- DOJ Order 2640.2E or the latest version for system certification and accreditation (http://10.173.2.12/dojorders/dojorders.php)

2.5.4 Technical Requirements

The Contractor's System shall meet or exceed the requirements identified in Attachment E, FOIA Requirements Matrix.

2.5.4.1 Security Requirements

Security requirements address the factors that protect the software from accidental or malicious access, use, modification, destruction, or disclosure. They also include requirements for maintaining an audit trail of changed data. Security requirements are established based on an assessment of the damage that may result if system security were compromised. Damages are classified as:

- Erasure or contamination of application data;
- Disclosure of Government secrets; and
- Disclosure of personal or privileged information about individuals.

Security requirements address the following areas to ensure the needed level of security is implemented based on the damage assessment.

- Physical and Environmental Controls – Physical protection in the facility housing the system application and subsystems such as: locks on terminals, physical barriers, and site access controls.
- Identification and Authentication – Determine access and accountability of users by authentication controls such as password protection, PKI digital certificates and biometrics. It

should describe the level of enforcement (network, operating system, application, data), and enforcement procedures.

- Personnel Security – Personnel security will determine security clearances and background checks needed for analysts, administrators and other specified user groups, and the level of access granted by duty assignment.
- Additional Security Requirements – Other security requirements may be determined in the areas of incident response, certification and accreditation policies, and security awareness and training.
- Audit Trails – Audit trails provide necessary information to support user accountability, detect security violations, track performance problems and flaws in applications. Audit requirements address the need for a security audit trail, including the types of data tracked for each activity, guidelines on level and the frequency of access to audit information, archival requirements, and usability preferences on reviewing audit trails.

2.5.4.2 System Reliability

System reliability addresses the need to ensure the overall reliability of thesoftware system upon delivery. Reliability requirements include: establishing the availability of the system (e.g. such as hours of operation), expected time to recover the system from an abnormal termination or disaster and system backup requirements.

System reliability is the ability of a system (or system component) to perform its required functions under stated conditions for a specified period of time. It is the probability that the system will correctly and completely process instructions without aborting. These requirements address the need to protect against the potential loss that may occur due to system failure, in terms of employee productivity and the complete or partial loss of the ability to perform a mission-critical function. In addition, these requirements address the minimum acceptable level of reliability for the system. The Contractor shall be responsible for the reliability of the application itself, while DOJ will be responsible for the reliability of the processing environment.

Recoverability is the measure of the ability to restore functions and data in the event of a failure. Recoverability requirements will utilize the following metrics:

- Acceptable time period between detection of system failure and restoration of system functionality.
- In the event of database corruption or data loss, the timeliness of the last backup of data.
- In the event that the system fails, the ability of the system to switch to an alternate server and resume operating.

System availability requirements establish mandatory times when the application will be available for use. Availability requirements will determine when maintenance may be performed and identify any peak processing periods where system unavailability is unacceptable.

2.5.4.3 Data Requirements

Data requirements address the areas of data retention and data currency.

- Data retention requirements address the length of time data must be retained and accessible, based on data archiving policies and user requirements.
- Data currency is a measure of the timeliness of data. Business needs will define required and preferred measures on the currency of data accessible to users.

2.5.4.4 Supportability

Supportability requirements address the factors that determine the ease of administration and maintenance, level of system customization, testability, and portability of the application to other host machines and/or operating systems. Supportability requirements also address the processes used to create the system components, such as coding standards, architectural styles, and design patterns.

2.5.4.5 Performance Requirements

Performance requirements address the expected user volume and capacity that the system must support. Additionally, they address the user's expected response time for queries, updates and screen navigation.

- User volume describes the number and type of users expected to use the system overall and concurrently.
- Capacity requirements address the expected volume of data and projected growth, in business terms.
- Response time describes the time to save, update and retrieve records from the database.
- Response time also describes the time to generate or refresh a system screen.
- Response time also includes the time to authenticate a user login.

2.6 System Users

2.6.1 User Profiles

The system must support different types of users, with each having different privileges and capabilities. The Contractor shall be responsible for ensuring that each user is given the appropriate access level as specified by the COTR.

Table 3 – User Profiles		
User Role	**Privileges**	**User Description**
System Administrator	Provides tier 2 support: performs database maintenance functions and all tasks related to the environment support and trouble shooting.	Users who manage the operation of the system and perform environment-related trouble shooting tasks.
Component System Administrator	Provides tier 1 support: Modifies the component staff's system access privileges, adds/deletes/ component system users and configures at the component level. Ability to perform all tasks allowed by lower access levels. Views existing records, creates new records, edits and deletes (archives) records as needed.	Component uses who manage the operation of the application and perform application-related trouble shooting tasks.
OIP Initial Request Staff	Views existing records, creates and modifies new records, edits, deletes and redacts records, as needed.	Process and review FOIA requests.
OIP Administrative Staff	Enters requests and appeals into the system and directs them to the appropriate staff member or other entity for action.	Initial creation and subsequent administrative maintenance of request and appeal records.
OIP Appeals Staff	Views existing records and other components' records, creates and modifies new records, edits and deletes records, as needed.	Process FOIA Appeals.

2.6.2 User Training

The Contractor shall train system administrators, OIP staff, and all other system users prior to the implementation of any FOIA Automation system. Training shall include instructional training and may include the development and maintenance of a training curricula and documentation as directed by the Government. **Specific training requirements will be described by the Government under individual BPA calls.**

Generally, core training shall include system training as well as business process trainingwith the Contractor preparing varying training curricula, as directed by the Government, depending upon the type of training required. The Contractor shall also provide supplemental/refresher training, as directed by the Government, in response to system upgradesor enhancements throughout the life of the BPA. The nature of the training will depend upon the number and complexity of any enhancements or new requirements to the system.

2.7 Performance Standards

The System shall be accessible to internal users no less than 99.99 percent of the time while the System is operational. However, the Contractor shall not be responsible if theSystem becomes inoperative, inaccessible, or non-responsive as a result of malfunction or limitations in the System due to the fault or negligence of the Government due tofactors external to the system that are the Government's responsibility (i.e., Government furnished equipment malfunction, network communications malfunction, etc.).

2.8 Reserved

2.9 System Development Life Cycle (SDLC) Tasks

Throughout the course of the project the Contractor willbe required to perform its work on the project in a manner consistent with the Systems Development Life Cycle (SDLC) methods and pocedures adopted by DOJ. Each of the BPA Call will describe in detail these SDLC processes with work elements tasks/steps and project deliverables that must be followed and prepared on the project. The project requires that the FOIA System be acquired and/or developed according to the guidance, principles, and practices set forth in the above-mentioned SDLC. Key elements of the SDLC related to this effort and required for this project are noted below.

2.9.1 Project Management Plan

Using the Department's standards and procedures as a basis, the Contractor shall adopt/develop a Project Management Plan (PMP) detailing its management procedures as they will apply to this effort. Revisions to the PMP shall occur as needed at the end of each phase. The PMP, whenpossible and practical, shall utilize the standards and procedures provided by the SDS PMO and will include processes for:

- Work Breakdown Structure (WBS) and Schedule Management
- Change Control Management
- Product Acceptance Management
- Communications Management
- Risk Management
- Security Management
- Resource Management, including organization chart, roles and responsibilities
- Financial Management

2.9.2 Project Plan

The Contractor shall prepare a Project Plan that provides a WBS and schedule of all work, deliverables and work products. The Project Plan will be updated at least every two weeks and an updated plan shall be submitted along with the bi-weekly status reports. The Project Plan shall contain:

- WBS reference numbers.
- Description of work to be performed (tasks).
- Resources required to complete the work, including name and position.
- Milestones, task relationships and interdependencies, and critical path.
- Time phased distribution of labor hours required to complete the work.
- Start and end dates (baseline and actual values).
- Hours required for completion (baseline and actual values).

2.9.3 Requirements Traceability Matrix (RTM)

The Contractor shall develop a Requirements Traceability Matrix (RTM). The RTM will provide a method for tracking the requirements and their implementation through the development and testing process. The RTM shall include each requirement in the matrix along with its associated source and reference number. As the project progresses, the RTM shall be updated to reflect each requirement's status. When the system is ready for system testing, the matrix shall list each requirement, where it is addressed in the system and what test(s) verify that it is correctly implemented.

2.9.4 Product Evaluation and Acceptance Test Plan and Test Report

The Product Evaluation and Acceptance Test Plan defines the approach, criteria and method to ensure that COTS, GOTS or other packaged software products proposed as the basis of the FOIA system conform to the technical requirements imposed on the new system by the DOJ operating environment and that any recommended software package appears adequate to satisfy known and future business, user and technical requirements without excessive modifications. In this task, proposed software capabilities will be demonstrated against known functional and systems requirements and a gap analysis will be prepared describing the customizations needed to meet established requirements. In addition, system operations and maintenance manuals will be reviewed and the effort needed to upgrade these materials to DOJ and project requirements shall be included in the gap analysis.

2.9.5 System Design Document

The Contractor shall produce a System Design Document (SDD). The SDD shall identify all relevant technical, product and operational details for in the architecture; define interface specifications; identify key data aggregates; and describe product customizations and configurations to fill known gaps and meet the established requirements.

2.9.6 Preliminary Design Review/Critical Design Review

Preliminary Design Review (PDR) is held during the Configuration phase to permit an interim review of initial engineering and design concepts to ensure that the proposed system meets with DOJ approval and satisfies the identified requirements. The PDR shall include:

- Functional Capabilities
- Proposed system and functional specifications (functional overview, interfaces, data constructs, dependencies and assumptions, risks, schedule checkpoints and interim milestones)
- Operational roles and responsibilities
- Performance objectives
- System platform characteristics
- Logical data model

The purpose of the *Critical Design Review (CDR)* is to review the detailed design of how the system will meet the defined requirements. The CDR shall reflect the maturity of the system design and provide a greater level of detail than the PDR. The review should demonstrate how the approach is consistent with the DOJ's Enterprise Architecture, and is adequately secure, robust and maintainable.

2.9.7 Implementation Plan

The Contractor shall develop an Implementation Plan that governs the implementation of the system for users in a production processing environment. Upon completion of the draft version of the Implementation Plan, the document shall be submitted to the COTR for review andapproval. The Implementation Plan shall at a minimum include a detailed WBS and Master Rollout schedule identifying all of the tasks that shall be performed during the rollout. The WBS shall also include a list of pre- and post-implementation tasks. All tasks must designate who is responsible for task completion -- the Government (by position– Component Name) or the Contractor.

2.9.8 Contingency Planning

The Contractor shall develop plans for responding to incidents and planning for contingencies that might impact the new FOIA system. At a minimum, the plan shall identify critical assets/resources, potential impacts resulting from unplanned incidents, recovery strategies, and system restoration priorities. The plan shall be submitted to SDS for review and approval. Incident reporting and contingency procedures shall be included in test plans approved for the project.

2.9.9 Security Planning

The Contractor shall support the preparation of a Security Plan (SSP) for the project that, at a minimum, shall include:

- Descriptions of the applicable system security requirements, system boundary, interconnections, interfaces, and strategy for performing the security certification
- Descriptions of the planned technical and non-technical security controls and change control processes.
- Rules of Behavior for personnel responsible for operations, support, and maintenance of the system, including consequences for its violation.

The Contractor shall support updates to the SSP throughout the system life cycle to identify changes.

2.9.10 System Test and Evaluation Master Plan

The Contractor shall develop a System Test and Evaluation Master Plan (TEMP) detailing individual test cases, the test conditions and expected results of each test case. Results of the testing will be provided to the SDS-designated testing coordinator for review and inspection. This plan, at a minimum, must demonstrate that the Contractor shall test all functional and systems requirements detailed in Sections 2.5 and Attachment E, Requirements Matrix, of this document including any additions/modifications agreed upon in the initial stages of the project and incorporated into the Requirements Traceability Matrix. For the purposes of this effort, SDS will require as many as four series of tests, including:

- **Initial System Testing** - Initial system testing will commence in the later stages of the Configuration Phase of the SDLC. This test, likely to be performed prior to moving software into the DOJ environment, will focus on the verification and validation of the standardized system to ensure the proper functioning of any customizations and that the full complement of required functional requirements have been implemented within the new system. System installation and configuration procedures will also be created during this activity in preparation for installation in a DOJ environment.

- **System Testing/Integration/Performance Testing**– This test will occur as the proposed software system is moved to the DOJ environment provided by SDS. The test will ensure proper installation and configuration of the software in the DOJ environment. In addition, this series of tests will address any requirements/processing variations specific to the various

components that will utilize the FOIA System, and will ensure the ability to satisfy required system interfaces/interactions in the DOJ environment.

- **User Acceptance Testing** – Subsequent to integration testing in the DOJ environment, the User Acceptance test is performed. During the task User Acceptance Test Plans are updated, test results are recorded and the Contingency Plan and Incident Response Plan are tested to ensure their accuracy and integrity at the Component level.

- **Security and Certification Testing**– While much of the documentation required for security and certification testing will be prepared by the Contractor in earlier phases, actual system certification will occur in the implementation phase. The requirements of certification testing are lengthy and are included as a separate section below.

In the Implementation Phase, DOJ shall use the System Test Plan as a primary basis for acceptance testing. The System Test shall test system functionality, userfeatures, and general performance characteristics of the system. Changes made due to errors or changes in user requirements will be reflected in the System Test Plan as additional test cases.

2.9.11 Test Readiness Review

The Test Readiness Review is held after the Configuration phase has been completed. Test plans will have been fully developed and updated and initial system testing at the Contractor's facility will have been performed. The purpose of the Test Readiness Review is to demonstrate that all configuration management procedures have been followed, and the system is ready for installation in the DOJ SDS environment and final testing prior to production implementation.

2.9.12 System Data Migration Plan

If directed by OIP, the Contractor shall develop a detailed plan for migration of required data from existing system data repositories to the new system.The Vendor will perform the data cleansing for the active data that is to be migrated. The data to be converted will include only current active records. The Contractor shall ensure that all data is accounted for and properly incorporated into the data structures of the new FOIA system. The Contractor shall also take appropriate measures to ensure original data in the existing systems are not destroyed or altered during the conversion as this system will be maintained for a lengthy period of time to ensure access to historical information.

2.9.13 Training Plan

The Training Plan provides the detailed approach, method, and plan for delivering FOIA training to users and DOJ technical support staff. The Training Plan will define the users who will require training (e.g., users and system administration), identify the training methods to be used (classroom, CBT, video, etc.), identify required help desk support functions and produce the user operating procedures and technical training documents needed to ensure proper system operations and support. System Security Awareness and Rules of Behavior will be integrated into the delivery of this training.

2.9.14 User Support Plan

The User Support Management Plan, Help Desk Management Plan, and the System Operation and Maintenance Manual (SOMM) are created during this activity. The User Support Management Plan identifies the methods, approach, and plan for establishing and managing help desk support and for producing user and administrator documentation for the system.

The Help Desk Management Plan provides guidelines for reporting, logging, tracking, managing, and

monitoring all reported trouble tickets, as well as the method for providing responses andsystems to users. The detailed plan for trend analysis and measurementof trouble tickets shall be defined in the Help Desk Management Plan for continuous improvement.

The System Operation and Maintenance Manual provides detailed procedures and steps for system operation, maintenance, and troubleshooting for system administrators.

2.9.15 Certify and Accredit the FOIA System

The Contractor shall support all Certification and Accreditation activities which will be conducted by the Government. The Contractor shall provide any information needed for the Certification and Accreditation process and shall follow up on any findings that arise in the process.

At a minimum, the Contractor shall use the following certification and accreditation standards and guidelines documents:

1. FIPS 199 Standards for Security Categorization of FederalInformation Systems
2. FIPS 200 Minimum Security Requirements for Federal Information and Information Systems
3. DOJ 2640-2E Information Technology Security
4. DOJ Telecom Network Security Concept of Operations DOJ Security Architecture
5. DOJ ITSS Standards and Guidelines
6. NIST Special Publications, including:

- NIST SP 800-37 Guidelines for Security Certification and Accreditation of IT Systems and referenced documents
- NIST SP 800-18 Guide for Developing Security Plans for Information Technology Systems
- NIST SP 800-30 Risk Management Guide for Information Technology Systems
- NIST SP 800-14 Generally Accepted Principles and Practices for Security Information Technology Systems
- NIST SP 800-27 Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
- NIST SP 800-34 Contingency Planning Guide for Information Technology Systems
- NIST SP 800-47 Security Guide for Interconnecting Information Technology Systems
- NIST SP 800-53 Rev 1 Recommended Security Controls for Federal Information Systems
- NIST SP 800-53A Techniques and Procedures for Verification of Security Controls in Federal Information Technology Systems.

2.9.16 Security Testing

The system shall be tested to ensure it meets all security requirements. Contractor shall respond to findings and shall fix any vulnerabilities that are discovered.

2.9.17 Operations Readiness Review

The Operational Readiness Review is held after successful completion of integration testing, user acceptance testing and the proper execution of C & A procedures. The purpose of the Operations Readiness Review is to demonstrate that the system has received accreditation, has a defined plan for implementation, and is ready to be deployed.

2.9.18 System Implementation

Prior to implementation, the application must be shown to be fully configured and functioning as

described both in this BPA and the Contractor's proposal, and fully customized, where applicable, to meet all BPA requirements as identified in this Statement of Work. Systems implementation shall not commence until C & A processes have been successfully completed, user acceptance testing and training tasks have been completed to the satisfaction of the COTR, data conversion has been approved by the COTR, and an ATO has been received. The Implementation will include:

- Implementation of production software and processes in the established SDS environment.
- Training of system users for each of the targeted offices.
- Converting and migrating all active FOIA data.
- Deploying the system in each of the targeted offices.

The successful completion of the FOIA implementation is a prerequisite to continuing further work associated with future phases of the FOIA system, in particular the departmentwide implementation.

2.10 BPA Management

2.10.1 General Requirements

The Contractor shall provide all management, administration, staffing, planning, scheduling, procurement, etc., for all items or services required by theBPA and/or BPA Call. This shall include, but is not limited to:

- All activities associated with recruiting and hiring staff, such asadvertising, screening applicants, interviewing, reference checking, etc;
- Screening and processing prospective contract staff to ensure that all Contractor employees used under this BPA meet personnel hiring and security clearance requirements;
- All activities associated with management of the Contractor's facilities that may be utilized, including obtaining space, equipment, furniture, supplies, maintenance, etc;
- Ensuring facilities used for the Contractor's performance of thisBPA meet all physical security requirements of the BPA;
- 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;
- Planning for and making all necessary arrangements to ensure that Contractor personnel performing field work have all necessary supplies and equipment by the time theyarrive at the site;
- 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;
- 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.;
- Tracking and reporting on Government-furnished materials, such as Government-furnished equipment and furniture. 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 lost or stolen while in the Contractor's safekeeping; and

- All activities associated with managing subcontractors, such as identifying and qualifying them, negotiating subcontracts, obtaining Government approval for their use, reviewing invoices, ensuring compliance with the security and other requirements of thisBPA, etc.

The above items shall be included in the pricing estimates for the applicable service.

2.10.2 Key Personnel

The positions listed below are considered key positions for this BPA. Individual BPA Calls may identify additional labor categories/persons as key personnel.

- Project Manager
- Lead System Developer
- Lead Business Analyst

Any individual performing work under the BPA and identified as a key personnel is subject to the following:

- Replacement of any key personnel is subject to the prior written approval of the COTR;
- Requests for replacement shall include a resume containing a description of position duties and qualifications of the individual proposed. The resume shall be of sufficient detail to demonstrate that the proposed individual is capable of performing his/her duties; and
- Contractor proposals to move any key personnel off theBPA or from one part of the BPA to another shall be submitted in writing at least 30 days in advance of the proposed move, and are subject to the approval of the COTR. This includes approval of the proposed replacement.

The Contractor's Project Manager shall meet with the COTR and/or the COTR's designee on a weekly basis to review scheduling, priorities, funding, performance issues, and other projectrelated matters. In addition, weekly and monthly status reports must be presented to the COTR to assess planned versus actual progress. There will be face-to-face status-specific meetings weekly and monthly, or as requested by the COTR, between the appropriate Contractor managers, members of the COTR's staff, and other Government officials. Brief written minutes for each of these meetings will be required; the minutes should be produced within two work days of the meeting, state all agreements reached, list all pending action items, and attach all relevant handouts used at the meeting. Minutes shall be distributed to all meeting attendees.

2.10.3 Training of Contractor Staff

The Contractor shall be responsible for providing trained, experienced staff to perform the work under this BPA, and for continuously monitoring, managing and controlling the work. The Contractor shall make its best efforts to retain staff that have gained experience on this BPA, and to minimize staff turnover.

The Contractor shall train its own staff so as to ensure that all personnel are able to perform their duties under the BPA and each BPA Call satisfactorily. For example, the Contractor shall train its own staff in system procedures. This may require staff training in the specific technology area- such as the system architecture, or database integrity. The Contractor shall also provide training for its staff should any System upgrades occur (new releases, patches, etc. of any system software product). Upon request, the Contractor shall furnish the COTR with formal documentation of the training provided to Contractor staff including testing tools for determining whether individual employees have achieved required competence levels. Training of contractor staff is not separately billable under this BPA.

In addition to job-specific or professional training, the Contractor shall ensure that its employees on this BPA are trained on "BPA-specific" issues such as DOJ ethics, standards of conduct, individual conflicts of interest, confidentiality requirements, DOJ security requirements, security clearance processes and terminology, the function of reporting, and the importance of quality control and quality assurance. Contractor managers shall also be educated in the terms and conditions of theBPA.

2.10.4 Quality Assurance and Quality Control

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 BPA for the duration of the BPA. Contractor shall stress to its staff the importance of quality control and quality assurance.

Within the specifications of the BPA, the guidance of procedures manuals, and the direction of the COTR, 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 BPA activities independently and shall exercise professional judgment and discretion in making decisions and recommendations for the successful completion of the activities. As appropriate, Contractor shall make suggestions to the COTR to improve operational procedures and shall obtain COTR approval prior to implementing any precedent-setting decisions.

The importance to the Department of quality control cannot be overstated. The Department is committed to quality work. Frequently, work must be performed under rigid time constraints without sacrificing attention to detail and quality. The Contractor must perform quality control reviews, as needed, for each functional area of the BPA. Without significantly slowing the flow of work, these quality control reviews should, to the extent possible, include reviews of valid samples of work at critical stages in the work flow to verify the accuracy of the work before proceeding to the next stages of work. The Contractor's reviews shall address the following:

- Ensure personnel are following all established guidelines and procedures; and
- Identify appropriate modifications to procedures manuals or other corrective actions to improve efficiency or remedy deficiencies.

After each quality assurance review, Contractor shall provide a written findings and recommendations report to the COTR.

2.10.5 Status Meetings

2.10.5.1 Weekly Team Status Meetings

The Contractor Project Manager, the Government Project Manager, and other key members of the Project Team as necessary will conduct a weekly status meeting. The weekly status meeting will review the project schedule, project costs, risks, current project activities, near-term project activities, resource requirements, outstanding issues, etc. for the preceding reporting period.

2.10.5.2 Monthly Executive Status Meetings

A monthly executive status meeting will be conducted by the Contractor Project Manager, the Government Project Manager, the executive sponsor and/or delegates and other key members of the Project Team, as necessary. The monthly status meetings will review the project schedule, project

costs, risks, current project activities, near-term project activities, outstanding issues, etc. for the preceding reporting period.

2.10.6 Management Reports

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.

In performance of this BPA, the Contractor shall use reporting guidelines established by the SDS Program Management Office including but not limited to the following:

2.10.6.1 Weekly Project Status Dashboard Report

The Contractor Project Manager shall produce a regular weekly project status report consistent with the requirements of the SDS PMO reporting guidelines.

2.10.6.2 Weekly System Status Report

The Contractor Project Manager shall produce a weekly Status Report for distribution and presentation one day prior to the Weekly Status Meeting. This report shall provide more detailed information on status, risks, issues and milestones than the weekly status report and will provide updated task estimates to complete and staff utilization summaries for the period.

2.10.6.3 Monthly System Status Report

The Contractor Project Manager shall produce a Monthly Status Report one day prior to the Monthly Executive Status Meeting. The Report shall review the project schedule, project costs, risks, current project activities, near-term project activities, outstanding issues, etc. for the preceding reporting period and provide a financial accounting of project cost to-date and estimates to complete.

2.10.6.4 Monthly BPA Summary Report

The Contractor Project Manager shall produce a summary reporton all BPA Calls issued under this BPA. Minimum content requirements are listed below. The COTR will approve the format of the 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 any BPA Call, as needed.

BPA Call number
DOJ component
Date order issued and amount
For each modification: date issued and amount
Funds expended and remaining
Estimated funds necessary to complete
Summary of accomplishments during the period and planned activities for the next period

In addition, each BPA Call will identify reports to be submitted to the ACOTR.

2.10.6.5 Weekly Production Status Report – Post-Implementation

At the commencement of production processing at the conclusion ofPhase 1, the Contractor shall report weekly on system and user issues associated with system operations. Reports describing system incidents (and their resystems), Help Desk activities, system and user administration activities shall be prepared and delivered to the SDS PMO. The specific details of this report shall be agreed upon as part of the Phase 1 Operations and Maintenance Support Plan.

2.10.6.6 Monthly Production Report– Post Implementation

A statistical and narrative report summarizing the activities and metrics noted above shall be prepared by the seventh calendar day of the month following the subject month of the report. As above, the specific details of this report shall be agreed upon as part of the Phase 1 Operations and Maintenance Support Plan and will include change requests, security incidents/issues, and quality control issues/proposed improvements.

2.10.6.7 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 thisBPA. The Contractor should note that this may include computer andother equipment, computer software, etc. To support this function, the Contractor shall conduct a quarterly review of all Governmentowned property in its custody and document and update these holdings. This 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. The report shall contain, at a minimum, the following information:

- Item type
- Item description
- Make and model
- Serial number
- DOJ inventory number
- Leased or purchased
- Month/Year invoiced, if purchased for DOJ
- Warranty/maintenance information
- Current location (building/room)
- Previous location or disposition
- Project for which originally acquired
- Acquisition cost (if known)
- Property Classification

2.11 Government Facilities

The SDS PMO is located in the Patrick Henry Building at 601 Suite 1300 D Street N.W. Washington, DC 20530 Suite 1300. OIP is located at 1425 New York Avenue N.W. Washington, DC 20530, Suite 11050. Status meetings will be conducted at OIP's offices unless otherwise instructed.

Technical work performed associated with this effort (e.g., programming, debugging, testing, etc.) can be performed at the DOJ Systems Development Services (SDS) located in the Patrick Henry Building Prior arrangements are required including the approval of the COTR and the assigned SDS Project Manager.

For the purposes of this effort, integration testing, security testing and certification, conversion data preparation, and user acceptance testing must be performed inside government facilities which will

include the SDS facilities within the Patrick Henry Building and data processing facilities managed by SDS but located in the DOJ's Rockville, MD data center facility.

The target data processing facility for the FOIA System will be the SDS facilities located within DOJ's Rockville data center facility. More information is available regarding these facilities in Sections2.3 and 2.14 pertaining to Technical Standards and Technical Environment.

2.12 Contractor Facilities

Any contractor and/or subcontractor facility(ies) that may be used to access, store or process FOIA system data must be equipped with appropriate security systems and protocols as described in Sections 2.5.4.1. If required, any costs to implement and maintain such security measures at contractor's facilities are the responsibility of the contractor and are not separately billable.

2.13 Manuals and Documentation

The Contractor shall develop and distribute user procedures manuals for each Component utilizing the FOIA system. Each manual shall be a complete guide to the performance of all activities associated with a particular function. The manuals shall progressively describe, in narrative fashion, each step involved in performing the activities. The manuals shall be divided into logical sections or chapters that can be used independently by personnel that perform a particular function. The manual for each Component shall contain a comprehensive table of contents and a comprehensive index. The manuals shall be provided to pertinent project personnel in a format that permits the incorporation of new instructions and revisions without the need to rewrite or reorder the entire manual. In addition, the contractor shall develop and maintain comprehensive system operations and maintenance/support manuals throughout the course of the project. Copies of all manuals shall be maintained at the DOJ's offices and kept up-to-date. Quantities and deliverable date of the soft and hard copy manuals shall be described in each of the BPA Call.

2.14 Operations and Maintenance of the FOIA system

While the DOJ will provide an operating environment and Data Center support personnel for the FOIA system, the DOJ will require software support, software maintenance, system administration training, and production performance monitoring support for the FOIA system from the Contractor throughout the life of the BPA. As stipulated by the BPA Call, the Contractor shall prepare and deliver a detailed Support and Maintenance plan for this effort. This plan will include change control management procedures, user procedures, help desk plans and system administration and management procedures for operations support and maintenance of the FOIA production system. A responsibilty matrix describing the roles and responsibilities associated with providing operation and maintenance support services to the FOIA is included as Attachment E, Responsibility Matrix.

2.14.1 Software Maintenance

The Contractor shall provide software maintenance including software fixes, patches and upgrades for all required application software components (including application specific database components) of the FOIA system for the duration of this BPA.

2.14.2 Hardware Maintenance

SDS through its relationship with OSS shall be responsible for hardware maintenance for hardware utilized for the FOIA system unless hardware has been provided by the Contractor. In these cases, Contractor shall also be required to provide hardware maintenance for the provided components for the duration of the BPA.

2.14.3 System Operations

Following the acceptance of the FOIA system implementation, Contractor shall be responsible for ensuring the new FOIA system is properly configured and running successfully in the SDS operating environment. Contractor shall be assisted by DOJ's assigned SDS project manager who will work with the Contractor's representatives and be responsible for ensuring the FOIA system receives proper systems administration support in the SDS environment, including: adequate server-based hardware and processing priorities, adequate data communications and system access services, operating system patches and upgrades as required and consistent with the upgrades applied to the FOIA application, back-up services and disaster recovery/contingency planning services if required.

The Contractor will be responsible for applying application software upgrades and maintenance, application-specific database management and maintenance services, system production incident and performance reporting as described in Sections 2.10.4 and 2.10.5 (BPA Management) of this document and ensuring proper systems administration services are provided by trained user technical staff and SDS personnel.

2.14.4 Configuration Management

The Contractor shall ensure proper change management and control of the FOIA system throughout the life of the BPA. This includes development and maintenance of a Configuration Management Plan (CMP) to manage all requests and changes to the system. The CMP should include a method for documenting, tracking, and managing change requests from inception through resystem. The Contractor will be responsible for tracking, managing, and controlling all change requests, problem reports, report requests, etc. In addition, the Contractor will provide a written analysis of the problem or request, an estimate of the time and cost to resolve the problem or request, and an analysis of the impact on the overall system, if any. All requests for changes not related to the immediate restoration of system services will be submitted for review and approval to the DOJ prior to initiating work on the correction or enhancement.

2.14.5 User Support/Help Desk

The Contractor shall support the provision of proper Help Desk support services to system users by: planning for help desk services for the FOIA system, training Help Desk support personnel and by providing Tier 3 support for questions and issues requiring extensive knowledge of the software application. The initial contact for problems with the FOIAsystem will be JCON and, as such, the Contractor will be responsible for preparing training materials and training sessions for JCON personnel. The second tier of Help Desk support is to be performed jointly byParticipating Components' technical representatives and SDS personnel. The Contractor will be responsible for resolving calls/incidents beyond the knowledge of OIPand the SDS team and in the future, participating components, for training these individuals in order to minimize the number of calls/incidents that require Tier 3 support directly from the Contractor. For further detail see Attachment B: Help Desk Escalation Workflow.

The Contractor shall be responsible for planning the coordination between the user support professionals and to ensure all calls are tracked, monitored and are resolved in a timely manner. The Contractor shall plan to provide access to qualified support personnel between the hours of 7am-7pm Eastern Time, Monday through Friday.

2.14.6 Technical Support Training

In preparing OIP and SDS personnel for the Help Desk support tasks described above and to ensure

effective knowledge transfer of the technical aspects of the FOIA system, the Contractor will be required to prepare and deliver technically-oriented training to at least eleven (11) OIP and SDS personnel. This training will include the user training components and user proceduresas detailed in the training plan described in Section 2.9.13 of this document. In addition, the Contractor's technical training will include user management and administration training, application administration training, proper system configuration and installation procedures, system recovery procedures and system change control procedures.

2.14.7 System Enhancements

The development of the FOIA system will occur in multiple phases. The primary objective of the initial phase is to develop a FOIA electronic tracking and processing system supporting OIP's operations. Additional functionality, users and interfaces will be provided in a planned future phases. Subsequent to the initial implementation of the FOIA system and in the initial support period, both DOJ and the Contractor may consider providing additional scheduled software updates, minor user-requested modifications and enhancements, and/or Contractor identified improvements in those cases in which the provision of additional functions and features can be provided in an expedited manner and cannot be easily deferred to a later release of the software (i.e., in future phases). The Contractor shall develop a Life Cycle Management Plan (LCM), in accordance with the DOJ SDLC, that will establish guidelines, activities, and schedules for planning, designing, developing, testing, and implementing future software releases and planning for the possibility of emergency releases to resolve system bugs or to incorporate mission-critical enhancements required prior to the next scheduled release date.

2.15 Implementation Tasks and Deliverables

The Contractor shall provide all management, administration, staffing planning, scheduling, procuring, etc. for all items and services pertinent to each Component's implementation. Each BPA Call shall outline implementation deliverables and due dates.

2.15.1 Component Implementation Analysis

The Contractor will be required to begin the analysis and development and deployment of the FOIA system for components based on requirements specific to the components as they are developed. The Contractor shall prepare a written Work Performance Plan for the Government to review and approve. The Contracting Officer's Technical Representative (COTR) shall work with the Contractor to develop a format for the plan. However, at a minimum, the plan shall detail how the work will be performed, including how the System shall be configured, integrated, tested, and deployed; the proposed project time frames and milestones, potential obstacles that may arise during performance; and recommended systems to these obstacles. The Work Performance Plan shall be submitted to the (COTR) within fifteen (15) calendar days of the BPA Call, and will ultimately be reviewed by the Department's Office of the Chief Information Officer, EnterpriseSystems Staff, Systems Development Service (OCIO/ESS/SDS).

2.15.1.1 Roles and Responsibilities

(a) The Contractor shall be responsible for:

- Developing the business capabilities and functional requirements for additional components.
- Conducting requirements-gathering sessions with the components' FOIA users and other identified user groups.
- Developing system enhancement plan and approach, including system recommendations.
- Developing a deployment approach and timeline for the components.

(b) The Government shall be responsible for:
- Facilitating requirements-gathering sessions.
- Reviewing and approving gathered business capabilities, functional requirements, and recommended systems.
- Reviewing and approving approach and timeline for subsequent phases.

2.15.1.2 Deliverables

The deliverables provided to the Government by the Contractorto include:
- Business capabilities and functional requirements for the components' deployment of the FOIA system.
- Approach and project plan for a component's deployment of the FOIA system.
- Recommended system for a component's deployment of the FOIA system

2.15.2 Project Planning

The Project Planning activity shall formally kickoff the FOIA Automation project with the Contractor. Existing artifacts developed by the government shall be reviewed with the Contractor and a project management plan/project schedule plan shall be established and agreed upon. If the contractor has proposed COTS, or similar, software the Contractor will demonstrate these products to the government and establish their appropriateness for the new FOIA Automation system. Finally, the functional requirements document will be confirmed and updated.

2.15.2.1 Roles and Responsibilities:

(a) The Contractor shall be responsible for:
- Participating in the kickoff meetings to review all government artifacts relatedto the FOIA Automation project;
- Reviewing, validating and updating the functional requirements provided by the government;
- Demonstrating the suitability of any COTS, or similar, software products proposed as part of the Contractor's system; and
- Developing a Project Management Plan (PMP) and a detailed project schedule for implementing the FOIA Automation project.

(b) The Government will be responsible for:
- Participating in the kickoff meetings to review existing artifacts;
- Providing and facilitating detailed analysis ofthe FOIA business model and current functional requirements;
- Reviewing and approving proposed software system for the FOIA Automation System;
- Reviewing and approving the PMP and FOIA Automation project plan/schedule; and
- Providing PMO materials and guidance to the Contractor's personnel

2.15.2.2 Deliverables

The deliverables provided to the Government by the Contractor include:
- Updated Functional Requirements Document.
- Software Product Acceptance Plan, Demonstration.
- Project Management Plan.

- Project Plan/Schedule.
- Updated (project-specific) PMO planning documents.

2.15.3 Development and Configuration

The Development activity will require the Contractor (onsite or offsite) to develop/customize the recommended system to fulfill the requirements outlined by FOIA and the OCIO team and to plan the professional implementation of the system at DOJ.

2.15.3.1 Roles and Responsibilities:

(a) The Contractor shall be responsible for:
- Developing a comprehensive design for the FOIA Automation system.
- Conducting design reviews with government representatives to secure approval of the system's overall design.
- Developing comprehensive planning documents for the following topics: implementation, contingencies, system support and maintenance, security, and certification and accreditation.
- Support for the certification processes.
- Providing updates on the status of development to the Government, possibly software demonstrations, if required to establish that the work is sufficient to pass the Test Readiness Control Gate.

(b) The Government will be responsible for:
- Providing and facilitating detailed analysis of the FOIA business model and current functional requirements – as needed.
- Participating in application demonstrations on behalf of the FOIA team.
- Reviewing development updates and approving change orders – as needed.
- Reviewing plans for accuracy and completeness.
- Test Readiness Control Gate approval.

2.15.3.2 Deliverables

The deliverables provided to the Government by the Contractor include:
- Updated Functional Requirements document
- Requirements Traceability Matrix
- Data Model
- System Design Document
- Software Customizations
- Implementation Plan
- Contingency Plan
- Support for Certification and Accreditation (C&A): the contractor shall provide all information needed for the C&A process as required, and shall complete action items and findings that result from C&A.
- Support and Maintenance Plan (including user support, Helpdesk)
- Regular Status Reports as noted in Section 2.10, BPA Management

2.15.4 Integration and Testing

Integration and testing activities are designed to ensure that the FOIA Automation system is performing in accordance with established requirements and can be used effectively and securely in

the DOJ processing environment. During this activity, the initial implementation participant(OIP) and OCIO/SDS will confirm that defined requirements are met by the new application. In addition, a data migration plan will be prepared.

2.15.4.1 Roles and Responsibilities

(a) The Contractor shall be responsible for:
- Developing testing approaches, test plans and test data for each specific set of tests – system, integration, user acceptance and possibly performance (refer to Section 2.9 – SDLC for more details)
- Conducting required tests, evaluating results and updating the system as required.
- Mitigating test failure points including keeping a detailed register of test results in accordance with change control procedures agreed upon with the government.

(b) The Government will be responsible for:
- Providing a test environment for system testing, integration testing, security testing and user acceptance testing
- Providing technical support to assist the Contractor in performing and completing each required test
- Reviewing and approving test approaches, test plans and test results
- Ensuring proper user participation in User Acceptance Testing
- Review and approval of data migration plan and the installation and configuration procedures manual

2.15.4.2 Deliverables

The deliverables provided to the Government by the Contractor include:
- System Test and Evaluation Master Plan
- Requirements Traceability Matrix Updates
- System Test Model, Test/Use Cases, Expected results
- System Test Results and Sign-off
- Integration Test Plan, Results and Sign-off
- User Acceptance Test Plan, Results and Sign-off
- System Installation and Configuration Procedures

2.15.5 Data Conversion and Migration

Data conversion and migration services includes changing electronic or hard copy data maintained in existing Department or Component legacy feeder systems formats into the FOIA system formats and then loading it into the system. Conversions may be required across operating systems and/or hardware platforms or between different databases and applications. It applies to application files and end-user database files. Activities may include data analysis and cleansing, creating file inventories, developing strategies and procedures for and conducting data conversions and ports, reconciling data and acceptance testing activities. The Contractor shall also develop procedures and propose methods for performing file migration with a minimum disruption to end users. At the discretion of the Government, the Contractor shall design, develop, test, and implement methods of verifying and documenting converted FOIA data. The Department or Components may use additional support contractors to assist with legacy system data extraction and cleansing.

2.15.5.1 Roles and Responsibilities

(a) The Contractor shall be responsible for:

- Developing data migration approaches, data migration plans, and data validation plan.
- Conducting and completing the data migration to the satisfaction of the DOJ.
- Validating the accuracy of the migrated data and support government in validation and acceptance testing.
- Mitigating of issues with migrated data.

(b) The Government will be responsible for:

- Providing information regarding existing data and data migration requirements.
- Providing the hardware environment for data migration.
- Providing technical support to assist the Contractor in performing and completing the data migration
- Reviewing and approving data migration approaches, data migration plans, and data validation plan.
- Ensuring proper user participation in User Acceptance Testing
- Review and approval of migrated data.

2.15.5.2 Deliverables

The deliverables provided to the Government by the Contractorto include:

- Data Migration Strategy
- System Data Migration Plan
- Data migration technical design
- Data migration testing and validation plan

2.15.6 Training

Formal training will be conducted to introduce theproduct to FOIA users and SDS technical support personnel. It is recommended that various user functions and technical support requirements be reflected in the development of training materials and curriculum. Additional information regarding user training requirements is provided in Section 2.6.2. Training requirements for technical and support personnel are provided in Sections 2.14.5 and 2.14.6.

2.15.6.1 Roles and Responsibilities

(a) The Contractor shall be responsible for:

- Developing training plans and approaches
- Developing training materials for all types of user, technical and support roles
- Developing training schedules
- Conducting multiple training sessions
- Developing user procedures manuals

(b) The Government will be responsible for:

- Reviewing and approving training approach and plans
- Reviewing and approving training materials
- Reviewing and approving user manuals
- Providing facilities for training sessions

- Ensuring proper user participation in training sessions
- Participating in scheduled training sessions
- Approving completion of training prior to system implementation

2.15.6.2 Deliverables

The deliverables provided to the Government by the Contractor include:

- Training approaches and plans
- Training materials
- User procedures manual
- Preproduction Training Report

2.15.7 Deployment

The deployment activity would require the Contractor to install and implement the developed/configured application within the DOJ production environment. In addition, the contractor would also provide support services to the DOJ user base and desktop support personnel as part of the initial start-up.

SDS, in cooperation with a Vendor Technical Point of Contact, will mitigate product issues and avoid misunderstandings and confusion about the product during customization and deployment. This will assist users early on in the learning process to understand the product, so better decisions can be made by OIP and SDS.

2.15.7.1 Roles and Responsibilities:

(a) The Contractor shall be responsible for:

- Supporting the DOJ technical C & A tasks including the development and approval of all supporting documentation
- Completing data migration and training tasks to the satisfaction of the DOJ
- Completing Application Installation in the production environment and Configuration Procedures
- With the assistance of DOJ representatives, installing the application across the user base within the DOJ environment and providing initial support

(b) The Government shall be responsible for:

- Providing the production processing facilities for installation of the new application
- Providing lists of required users/requirements by user
- Reviewing and approving data migration and training efforts
- Facilitating DOJ technical C & A activities
- Conducting Operations Readiness Review
- Installation assistance technical support
- Acceptance of installed application

2.15.7.2 Deliverables

The deliverables provided to the Government by the Contractor include:

- Updated Requirements Traceability Matrix
- Approved Data Migration Report
- Approved Training Report

- Completed Application Installation and Configuration Plans/Documents
- Application installed and operational in DOJ environment

2.15.8 Operations and Maintenance

The Operations and Maintenance activity will require the Contractor to work in conjunction with the DOJ to provide support and maintenance services to user and technical personnel while the system is in use at DOJ. Refer to Section 2.14, Operations and Maintenance, of this document for specific details. The support option is for the term of the BPA and subsequent BPA Calls.

2.15.8.1 Roles and Responsibilities

(a) The Contractor shall be responsible for:
- Developing Operations and Maintenance Plan
- Providing support and maintenance functions for the new replacement application as defined in Section 2.14 of this document
- Tracking and reporting operations and maintenance activities/issues as described in Section 2.10.6 of this document
- Providing support across the user base for initial use

(b) The Government shall be responsible for:
- Reviewing and approving Operations Support and Maintenance Plan
- Reviewing and approving Production Status Reports
- Other tasks in support of a comprehensive operations support effort as described in Section 2.14 of this document.

2.15.8.2 Deliverables

The deliverables provided to the Government by the Contractor include:
- Updated Operations Support and Maintenance Support Plan(s)
- Weekly Production Status Reporting (See 2.10.6.5)
- Monthly Production Report (See 2.10.6.6)

2.15.9 Other Related Services

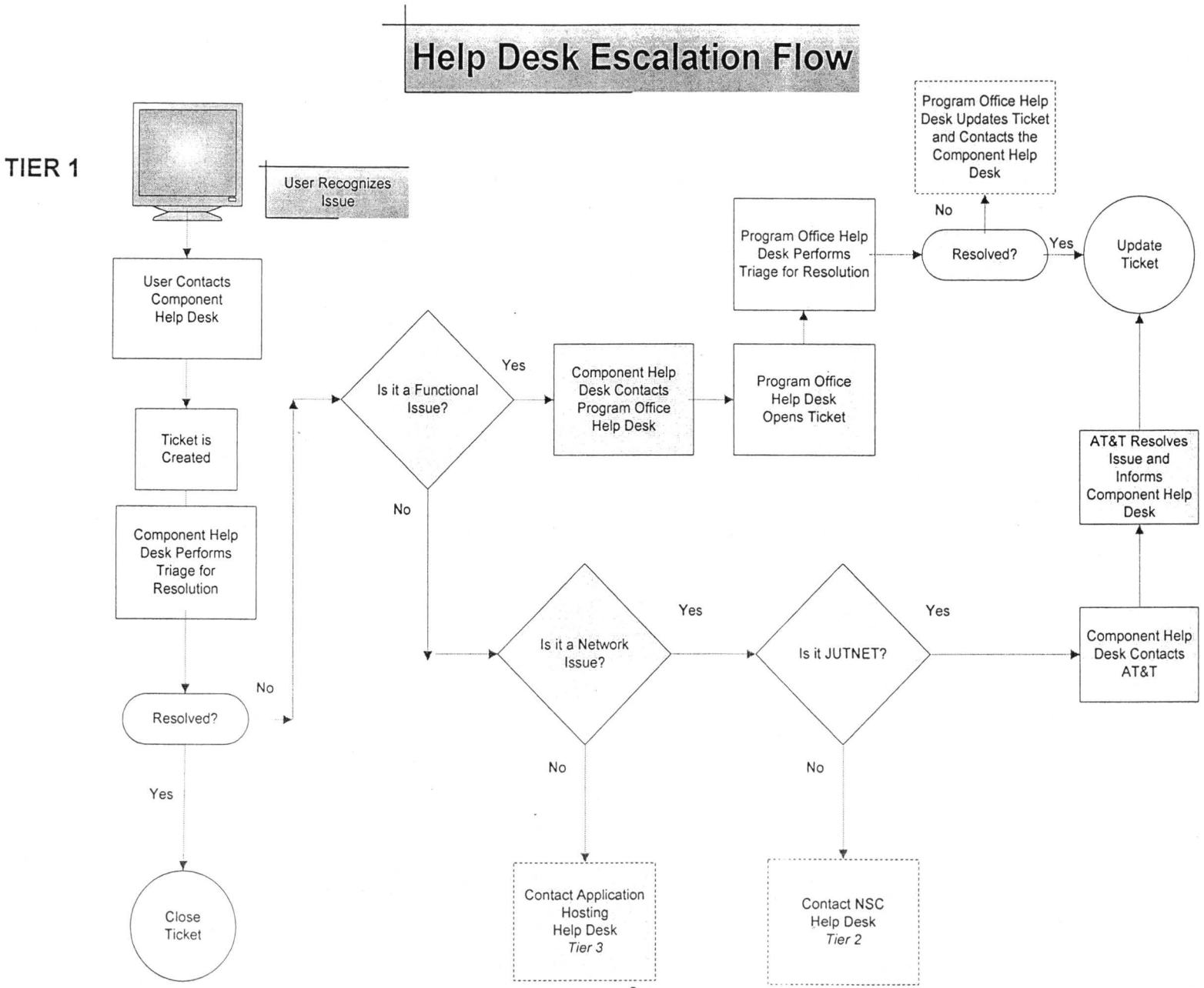
There may be other related FOIA, project management, or information technology professional services required for the successful accomplishment of the FOIA system implementation. Examples include research, analysis, and presentations. At the discretion of the Government, the Contractor shall facilitate briefings and/or work groups consisting of Government subject matter experts and/or Component representatives. In these instances, the Contractor may be expected to have prepared for the topic of discussion by researching current processes and existing laws and/or federal regulations or guidance. Services may also include security-related work. The Contractor may work with other SDS support contractors, Components and their support contractors, and an IV&V support contractor.

3. Deliveries and Performance

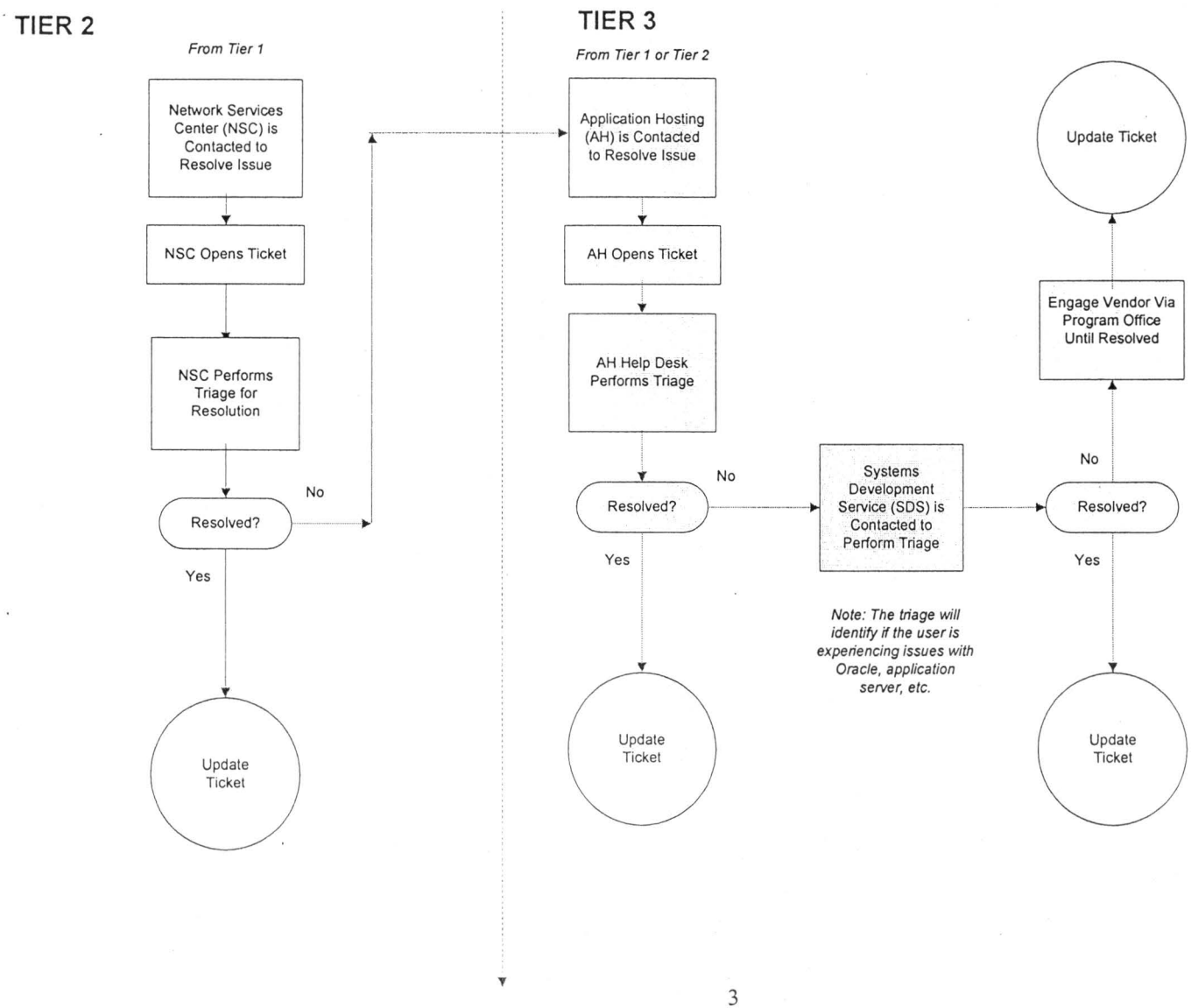
3.1 BPA Term

The term of this BPA is from the date of award through five years from date of award, subject to the Contractor maintaining and/or renewing its GSA, FSS contract and a determination by the Administrative Contracting Officer that this BPA is still considered the best value.

Attachment B



Help Desk Escalation Flow



ATTACHMENT C

U.S. Department of Justice

Justice Management Division - Systems Development Services

Development Environment Infrastructure As-built

Final Release <TBD>

Version 1.0

Draft

Prepared for:

U.S Department of Justice

JMD/SDS

Revision History

Revision	Date	Revised By	Notes
0	3/2/2007	Kdong	Initial Draft

Table of Contents

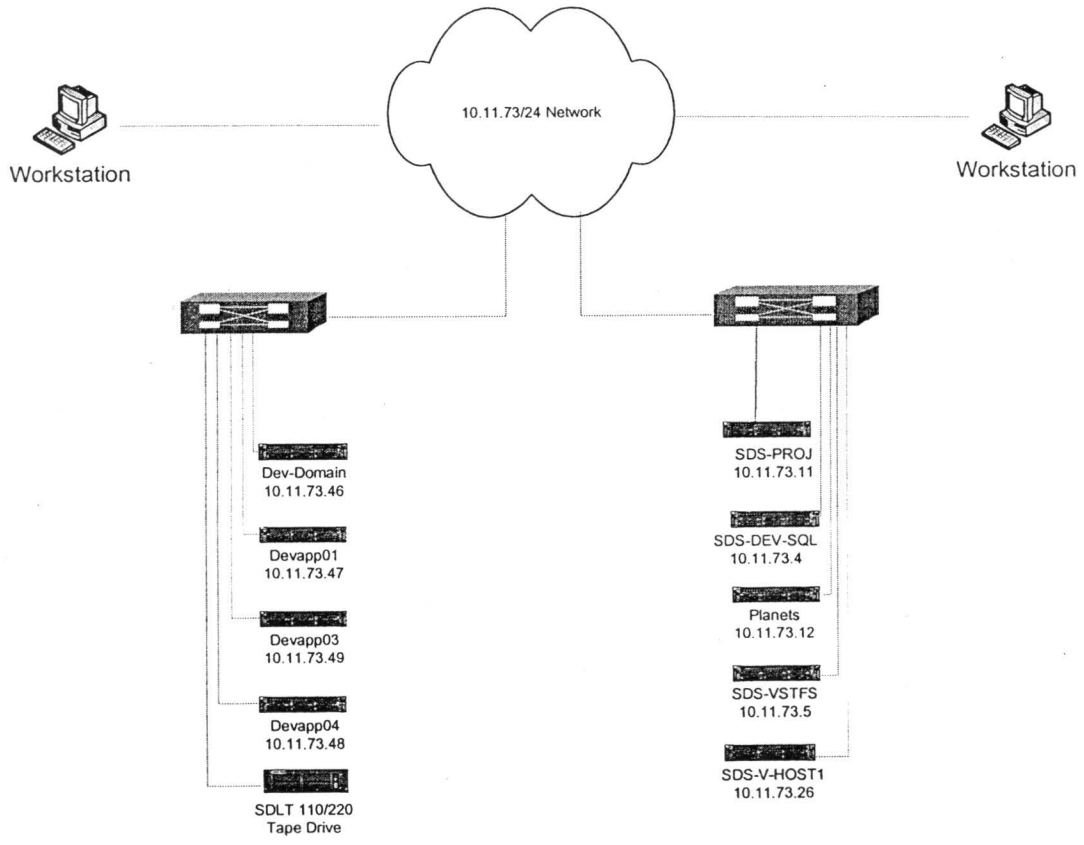
1 Introduction

The Systems Development Service (SDS) is responsible for the planning, coordination and facilitation of application development, maintenance and operation activities. SDS maintains and operates its own development environment to facilitate software development. This development environment consists of servers and workstations residing in 10.11.73/24 subnet of the JCON network and is capable of supporting at least 20 developers working on the same project simultaneously.

2 Networking

2.1 Network Diagram

SDS Development Environment
Network Diagram 3/2/07



2.2 Connectivity

Servers are connected to SDS Development network (subnet 10.11.73/24) via the Cisco switch which is connected to the room's patch panel. All servers will participate in SDS-JMD domain as domain member server.

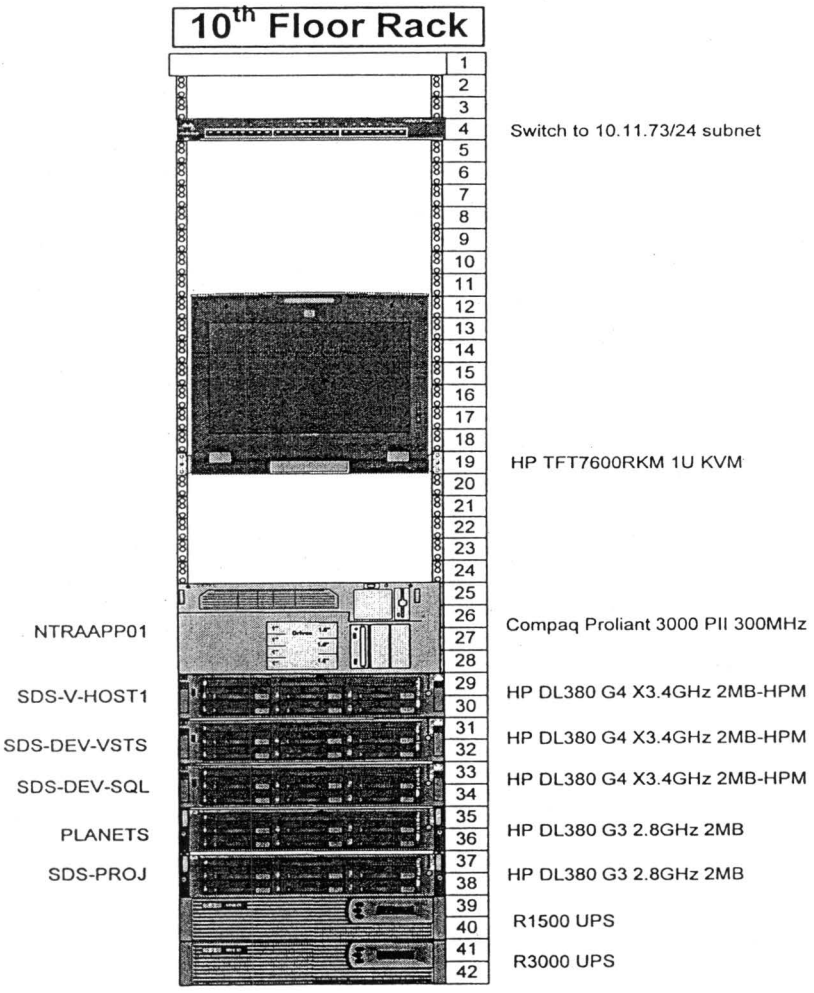
3 Hardware

3.1 Rack Location in 10th Floor, PHB

3.1.1 Rack Layout

Rack was installed in conformance to standards.

All equipment was labeled on the front of each device.

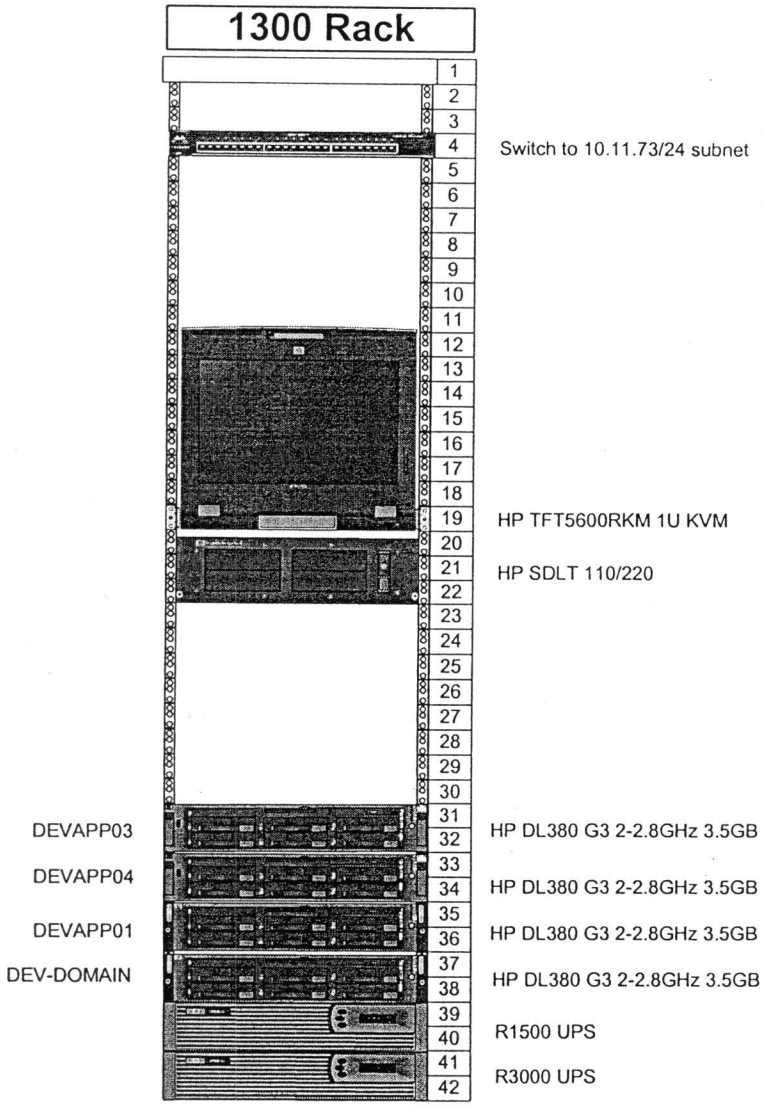


3.1.2 Server Specifications

Server Name	Hardware	Software	Applications
SDS-PROJ	Compaq Proliant DL380 G4 2 P3.4G Processors 2 GB memory 160 GB HD	Windows 2003 Server, SP1 MS Project Server 2003 Windows Sharepoint Services	Project server and WSS
PLANETS	Compaq Proliant DL380 G4 2 P3.4G Processors 2GB memory 160 GB HD	Windows 2003 Server, SP1 MS Virtual Server	Virtual Machine
NTRAAPP01	Compaq Proliant 6500 4 PIII500M Processor 4GB memory 72 GB HD	Windows 2000 Server , SP4	Oracle Forms
SDS-DEV-SQL	HP DL380 G4 HPM 2 X3.4G Processors 12G memory	Windows 2003 Server Microsoft SQL 2005 Server	SQL 2005 db instance SQL 2005 Analysis Services
SDS-VSTFS	HP DL380 G4 HPM 2 X3.4G Processors 8G Memory	Windows 2003 Server Visual Studio Team Foundation Server	SQL 2005 Reporting Services
SDS-V-HOST1	HP DL380 G4 HPM 2 X3.4G Processors 8G Memory	Windows 2003 Server Microsoft Virtual Server 2005	Virtual Host for Test Environment

3.2 Rack Location in Suite 1300, PHB

3.2.1 Rack Layouts



3.2.2 Server Specifications

Server Name	Hardware	Software	Applications
DEV-DOMAIN	Compaq Proliant DL382 1 Pentium 2.8G HT, 3.5 GB Memory 218 GB HD	Windows 2000 Server, SP4 Veritas Backup Exec 8.x CA eTrust Antivirus v7.1.192	AD, DNS, file share, Backup Server
DEVAPP01	Compaq Proliant DL380	Windows 2000 Server, SP4	WSUS, MS SQL Server

Server Name	Hardware	Software	Applications
	G3 2 P2.8G Processors HT 3.5 GB memory 64 GB HD	CA eTrust Antivirus v7.1.192 IIS 5.0 SQL Server 2000	
DEVAPP04 *Rational Server*	Compaq Proliant DL380 G3 2 P2.8G Processors HT 3.5 GB memory 218 GB HD	Windows 2000 Server, SP4 CA eTrust Antivirus v7.1.192 Rational	Rational software
DEVAPP03 *JRun Application Server*	Compaq Proliant DL380 G3 2 P2.8G Processors HT 4 Processors 3.5 GB memory 218 GB HD	Windows 2000 Server, SP4 CA eTrust Antivirus v7.1.192 IIS 5.0 Jrun 4.0 JReport 7.0 Oracle 9.2 client Java 2 Runtime SE v1.4.1_02 **Microsoft .Net Framework 1.1/Hotfix**	• AAGA-Dashboard • Dashboard • ADS • JACCS • JReport
SDS-DEV-DNS	Compaq Proliant 3000 1 PII300M Processor 320MB memory 12 GB HD	Windows 2000 Server, SP4 CA eTrust Antivirus v7.1.192	AD, DNS

4 Software

4.1 Database

The following relational database are supported on development environment:: Microsoft SQL Server 2000 and 2005, Oracle

4.2 Web

The following web servers are supported on development environment: JRun and Tomcat for Java EE development. IIS for Microsoft ASP and ASP.Net development

4.3 Other

Version Control - Rational ClearCase and Visual Studio Team Foundation Server
Data Modeling – Rational Rose and Visual Studio 2005
Performance Testing – Rational Robot and Visual Studio Team Foundation Server
Project Management – Microsoft Project Server 2003
Collaborative Tool – Microsoft Sharepoint Services

5 Server Management and Back Up

All servers are managed via Active Directory and domain policy. All security patching is done by Windows Server Update Service automatically. Backing up of the server is performed by HP StorageWorks SDLT 110/200 tape drive located in PHB 1300. Incremental backups are performed nightly and full backups are done once a week on the weekends.

U.S. Department of Justice

Justice Management Division - Systems Development Services

ESHP High Level Design

Final Release <TBD>

Version 1.0

Draft

Prepared for:

U.S Department of Justice

JMD/SDS

Revision History

Revision	Date	Revised By	Notes
1.0	3/8/2007	PDesRoches and JGodman	Initial Draft

Table of Contents

1 Introduction

The Enterprise Solutions Hosting Project (ESHP) provides a standard application hosting infrastructure for Systems Development Staff (SDS) and other Department of Justice (DOJ) components. The hosting environment is designed to provide a highly available, scalable, and flexible environment that supports several platforms. The architecture leverages existing and planned infrastructure and resources, thus allowing maximum benefit and lower costs.

The goal for ESHP is to create a standard hosting infrastructure for SIAS applications and eventually any DOJ application. The ESHP Vision:

- Deliver hosting as a service
- Reduced effort and rapid time to deployment
- Higher availability
- More manageable
- Lower Total Cost of Ownership

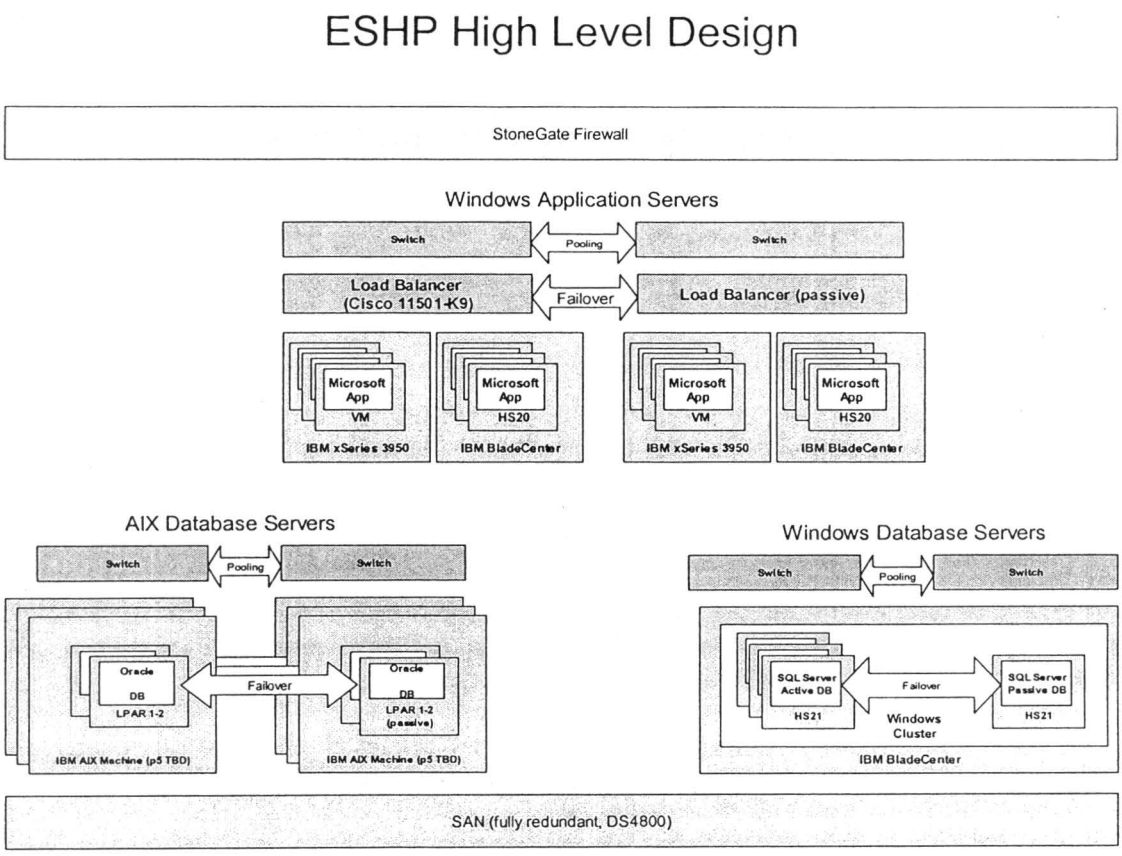
ESHP was developed jointly by SDS and the Operations Services Staff (OSS) who met to combine a set of joint requirements that would be consistent with CIO's Enterprise Architecture. The eventual full scope of ESHP would include High, Moderate and Low service levels that could accommodate all DOJ application requirements.

1.1 Current Scope

The ESHP design currently covers the Moderate level service offering only. As such, it is implemented in the Justice Data Center in Rockville only. There is currently no multi-site capability, however this may be offered in the future for the High level service offering.

Load balancers shown in the High Level Design Diagram below provide coordinated pooling redundancy ("load balancing") for all applications. SAN and network design components (other than switches and load balancers) are not shown at this time, but full intra-site redundancy will be implemented.

1.2 High Level Design Diagram



2 Platforms Supported

2.1 Application Platforms

At this time, the ESHP Moderate service level offering supports only one application operating system platform: Microsoft Windows Server 2003, in both Standard and Enterprise editions. Applications running on Windows Server 2003 may run on one of two primary platform choices: .NET or J2EE.

2.1.1 Microsoft .NET Application Platform

For .NET applications, a standard configuration of Microsoft Internet Information Server 6.0 plus all associated components (standard to the OS) is offered. Additionally, any custom .NET code or other Windows code may be installed on the application server.

2.1.2 IBM WebSphere J2EE Platform

For J2EE applications, a standard configuration of IBM WebSphere is installed on Windows Server 2003, including all associated WebSphere components, and any included Windows OS

components. Additionally, any custom J2EE code or other Windows code may be installed on the application server.

2.2 Database Platforms

At this time, the ESHP Moderate service level offering supports two database operating system platforms: IBM AIX and Microsoft Windows Server 2003 Enterprise. Oracle database server is offered on the AIX platform, which Microsoft SQL Server is offered on the Microsoft Windows platform.

2.2.1 Oracle

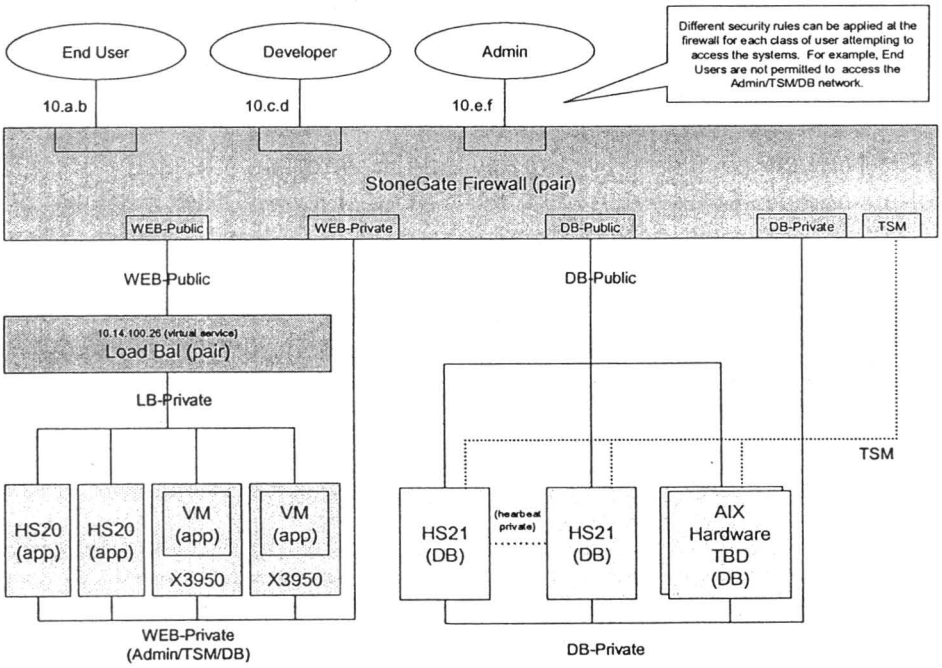
Oracle 9i and 10g is offered as a database platform running on AIX for ESHP applications that require this database platform. High availability is achieved via IBM HACMP clustering, with a fully redundant AIX server setup as a hot standby for zero-performance-loss failover in the event of server failure. Database storage is exclusively SAN-based.

2.2.2 Microsoft SQL Server

Microsoft SQL Server 2000 and 2005 is offered as a database platform running on Microsoft Windows Server 2003 Enterprise for ESHP applications that require this database platform. High availability is achieved via Microsoft Cluster Services, with N+1 clustering for zero-performance-loss failover in the event of any single server failure, and moderate performance impact failover in the event of multiple server failures. Database storage is exclusively SAN-based.

3 Networking

3.1 Network Diagram



3.2 Connectivity

3.2.1 End User to Application

End users will access ESHP applications through the StoneGate firewall on the WEB-Public network segment, to the load balancer virtual service address. The load balancers will route the web request to the appropriate application server on the LB-Private network. The application servers can then communicate over the WEB-Private network through the firewall, to the DB-Public network and into the database server.

3.2.2 Developer/Admin to Application

Developers and administrators will access console and other functionality on application servers through the firewall via the WEB-Private networks.

3.2.3 Developer/Admin to Database

Developers and administrators will access console and other functionality on database servers through the firewall via the DB-Private networks.

3.2.4 Backup

TSM backup will be performed for database servers on the TSM network. TSM backup will be performed for application servers on the WEB-Private network.

3.3 Firewalls

Firewall configuration and rules will be configured on the StoneGate devices that have been configured for the ESHP environment. In general, all ESHP web application traffic will be permitted through the firewall on a single SSL (port 443) virtual service running on the load balancers.

3.4 Load Balancers

Two Cisco 11501-K9 load balancers will support the overall ESHP environment, providing layer 7 switching services to the applications. The general load balancer configuration for the ESHP environment will be to perform SSL termination on the load balancers, and switch application traffic to each ESHP application's server pool. Applications will be identified through an URL path that begins with the main URL for ESHP (https://justapps.doj.gov) and includes a unique path for each application. For example, an application with the identifier "MYAPP" would be accessed at https://justapps.doj.gov/myapp/.

4 Hardware

Server hardware, network, SAN, power and facilities are provided by the Application Hosting Branch (AHB) at the Justice Data Center (JDC) in Rockville, MD. Current Design and as-built documentation will be maintained within various groups at the JDC.

4.1 Application Servers

Following the ESHP architecture, applications can be installed on Virtual Machines (VM) or dedicated IBM HS-20 blade servers running Windows Server 2003 Server Standard Edition.

4.1.1 Blade Server Environment

Windows Server 2003 Enterprise edition is installed on 12 IBM HS20 blade servers. Additional servers can be added to the environment as required.

Blade Type	Processor					Operating	
	#	Speed	RAM	NIC	FC	System	Applications
HS20	2	3.2 GHz	4 GB	2	2	Win 2003 ES	IIS version 6
HS20	2	3.2 GHz	4 GB	2	2	Win 2003 ES	IIS version 6
HS20	2	3.2 GHz	4 GB	2	2	Win 2003 ES	IIS version 6
HS20	2	3.2 GHz	4 GB	2	2	Win 2003 ES	IIS version 6
HS20	2	3.2 GHz	4 GB	2	2	Win 2003 ES	IIS version 6
HS20	2	3.2 GHz	4 GB	2	2	Win 2003 ES	IIS version 6
HS20	2	3.2 GHz	4 GB	2	2	Win 2003 ES	SharePoint Portal
HS20	2	3.2 GHz	4 GB	2	2	Win 2003 ES	SharePoint Portal
HS20	2	3.2 GHz	4 GB	2	2	Win 2003 ES	WebSphere
HS20	2	3.2 GHz	4 GB	2	2	Win 2003 ES	WebSphere
HS20	2	3.2 GHz	4 GB	2	2	Win 2003 ES	WebSphere
HS20	2	3.2 GHz	4 GB	2	2	Win 2003 ES	WebSphere

4.1.2 Virtual Server Environment

VMs will be hosted on at least two physical servers (IBM x3950) within a VMWare cluster. Although the VMWare cluster will be configured with the High-Availability option, layer 7 (application) load balancing will be the primary method for ensuring system availability.

Server Type	Processor #	Processor Speed	RAM	NIC	FC	Operating System	Applications
X Series 3950	8 Dual Core	3.2 GHz	64 GB	4 Aggregated	2 Aggregated	Windows 2003 ES on VMware ESX	IIS version 6, Oracle 9is, WebSphere, .NET
X Series 3950	8 Dual Core	3.2 GHz	64 GB	4 Aggregated	2 Aggregated	Windows 2003 ES on VMware ESX	IIS version 6, Oracle 9is, WebSphere, .NET

4.2 Database Servers

4.2.1 MS SQL Server Environment

SQL Server 2000 and 2005 is installed on four IBM HS21 blade servers. Additional servers can be added to the cluster or a new cluster as required. Microsoft Cluster service will be leveraged for high-availability.

Blade Type	Processor #	Processor Speed	RAM	NIC	FC	Operating System	Applications
HS21	2	3.2 GHz	8 GB	4	2	Win 2003 ES	SQL Server 2000
HS21	2	3.2 GHz	8 GB	4	2	Win 2003 ES	SQL Server 2005
HS21	2	3.2 GHz	8 GB	4	2	Win 2003 ES	SQL Server 2000
HS21	2	3.2 GHz	8 GB	4	2	Win 2003 ES	SQL Server 2005

4.2.2 Oracle Environment

Oracle will be installed on two IBM series p5 595 series servers running AIX using HACMP LPAR failover for redundancy and high-availability. Additional LPARS can be added as required.

	Processor		RAM	NIC	FC	Operating System	Applications
	#	Speed					
LPAR 1	0.7	1.9 GHz	8 GB	N/A	N/A	AIX 5.3	Oracle 9i
LPAR 2	0.7	1.9 GHz	8 GB	N/A	N/A	AIX 5.3	Oracle 9i
LPAR 3	0.7	1.9 GHz	12 GB	N/A	N/A	AIX 5.3	Oracle 10g
LPAR 4	0.7	1.9 GHz	12GB	N/A	N/A	AIX 5.3	Oracle 9i
LPAR 5	0.7	1.9 GHz	12GB	N/A	N/A	AIX 5.3	Oracle 9i
LPAR 6	0.7	1.9 GHz	12GB	N/A	N/A	AIX 5.3	Oracle 9i

5 Management Services

The ESHP environment will include standard services provided by the JDC. This includes providing Backup and Monitoring services. IDS, anti-virus, and patching services will also be provided by the JDC as outlined in security policy, certification and accreditation documentation, and ESHP service level agreements.

5.1 Backup

Standard nightly backups will be completed on all servers to include all local volumes and data associated with server SAN backup devices. Backup media retention will comply with DOJ backup standards and specifications provided in system certification and accreditation documentation.

Database servers and associated SAN devices will be backed up using an agent capable of backing up SQL server without requiring that the database be taken offline. Backups will only be performed during the standard backup window specified in the SLA.

5.2 Monitoring

System monitoring shall be provided by the JDC. This includes monitoring for network, server, and application failure. Where available, SNMP services will be leveraged to send traps to a centralized JDC monitoring system.

The JDC will be responsible for notifying persons responsible for failure or decreased system capacity/response of the system as outlined in the certification and accreditation and/or service level agreement for the ESHP environment.

ATTACHMENT E

United States Department of Justice (USDOJ)
Freedom of Information Act (FOIA) Automation System

Requirements Matrix

This Requirements Matrix serves as the basis for the Self-Certification process that is required as part of the Offeror's Technical Proposal. Offeror must complete the Requirements Matrix by placing the appropriate Requirement Code (Requirement Priority Codes, Requirement Vendor Response Codes or Level of Effort Response Codes) in the applicable column (4, 5 or 7) for the Functional Baseline, Technical Baseline and System Deployment & Support Tabs. Completed Matrix must be submitted with Offeror's proposal in order to be considered for award.

Upon Contract Award, this Requirements Matrix will become part of the resulting Contract.

To complete the self certification, Offeror must fill in the following three tabs (Functional Baseleine Requirement; Technical Baseline Requirements and System Deployment & Support Requirements) with Requirement Priority Codes, Requirement Vendor Response Codes and Level of Effort Response Codes. Definitions of these codes are below.

At the time of Award, the following "Critical" technical requirements **must** be met:
Technical Baseline Requirements: PE-1, PE-2 and PE-3
Systems Deployment & Support: SDS 12, 13, 14, 15, 18, 27
All other "Critical" Technical and "Critical" Functional requirements must be met following the User Acceptance Testing.

I. Requirement Priority Code

Code	Priority	Description
D	Desirable	The requirement is desirable and would enhance the reengineered process and may be met at the time the FOIA solution is implemented.
C	Critical	The requirement is critical to the success of the FOIA solution. Critical to be met at either baseline or system deployment.

II. Requirement Vendor Response Codes

A. Functional and General Requirement Responses

Code	Response	Description
0	Not Feasible	The requirement cannot be met by the Software Product, a 3rd party product is not available, and modification with vendor tools/custom programming is not recommended.
1	3rd Party Product Recommended	The requirement cannot be met satisfactorily by the software product, but a 3rd party product is available that can meet the requirement. Specify product in the Explanation column. Also indicate if an interface or API exists between the two products.
2	Targeted in Future Release	The requirement cannot be met in the current release, but is under development for a future release of the Software Package within 12 months. Specify the release number and planned release date in the Explanations column.
3	New Functionality Using Vendor Supplied Tools/ Custom Programming	Modifications required to meet this requirement involve development of new functionality using vendor supplied or other programming tools. Indicate in the Explanations column if such modifications would involve changes to any product source code and/or impact implementation, software upgrades, releases or builds or software maintenance.
4	Customization to Existing Objects Using Vendor Tools	Modification to existing objects (screens, tables, etc.) using vendor supplied tools is required to meet this requirement. Indicate in the Explanations column whether these modifications would include: addition of fields to existing screens and tables, changing field definitions/names, entering or attaching program logic to existing objects. Indicate if such modifications would involve changes to any product source code and/or impact implementation, software upgrades, releases or builds or software maintenance.
5	No Modification Required/ Table Driven Set-up	No modifications, customizations, or enhancements are required for the delivered software package to meet this requirement. Table values or other configuration set-up may be required.

B. Technical and System Deployment & Support Requirement Responses

Code	Response	Description
0	Not Feasible	The requirement cannot be met by the Software Product, a 3rd party product is not available, and modification with vendor tools/custom programming is not recommended.
5	Requirement Satisfied	The vendor or the delivered software product(s) satisfies the requirement.

III. Level of Effort (LOE) Response Codes

Code	Description
1	One week or less of effort
2	One to two weeks of effort
3	Two to three weeks of effort
4	Three to four weeks of effort
5	Five or more weeks of effort

LOE Response assumes a single, full time equivalent technical resource with appropriate skills and experience.
Weeks are calculated from date of award.

Functional Baseline Requirement

ID	Category	Requirement Description	Priority Code	Vendor Response	Name of Product, Release & Module	LOE to Obtain 100% Fit	Explanation
1.1	System/General	Processing and searching will be handled electronically. The system shall be capable of searching by various search criteria such as: requester name, subject name, subject matter, FOIA control number, Division file number, and more (to be defined at the detailed design phase).	C				
1.2		Authorized and assigned staff will have full access to the system: view, add, update, and delete data.	C				
1.3		The system shall have the ability to track initial requests by various types, including FOIA, Privacy Act (PA), Mandatory Declassification Review requests, and Presidential Records Act requests. The type shall be configurable to the components' needs.	C				
1.4		The system shall have the ability to identify initial requests that are broken into smaller requests and be able to aggregate them together for fee charging purposes.	C				
1.5		The system shall allow for note-taking at any stage of the process. It shall allow user to input notes and provide a time stamp and note history for each request.	D				
1.6		The system shall provide a centralized database for files and documents related to each request.	C				
1.7		The system shall provide the capability to telework.	C				
1.8		The system shall save addresses and provide capability to retrieve addresses for reuse and modify or update, as necessary.	C				
1.9		The system shall provide the capability for a status inquiry regarding a request. The system shall keep track of cases and their progress in the process.	C				
1.1		The system shall have the ability to interface with industry standard Document Management Systems.	D				
1.11		The system shall have the ability to accept an eform or an electronic version of a request.	C				
1.12		The system shall allow a requester to check the status of their request electronically.	C				
1.13		The system shall be able to support all the requirements at the component level, and should allow for component-level configuration. Also, the system shall allow for different workflows for different components.	C				
1.14		The system shall be capable of allowing users and reviewers to electronically redact documents responsive to requests, place notes on responsive documents, and generate standard and ad hoc reports.	C				
1.15		The product vendor shall update or upgrade versions and release new versions incorporating any and all new statutory and regulatory requirements related to the FOIA/Privacy Act, applicable to the system. Vendor shall work with agency to meet new compliance requirements in accordance with guidance issued by the Office of Information and Privacy. Software upgrades shall occur within 30 days or another agreed upon time period from the issuance of guidance.	C				
1.16		The system shall be able to be integrated with existing database systems and applications (such as Intranet Quorum). The system shall have the ability to generate notifications and integrate with Outlook calendar.	D				
1.17		The system shall be compliant with Section 508 of the Rehabilitation Act.	C				
1.18		The system shall allow for expansion for possible future tracking needs, to include additional categories other than just initial requests, appeals, and DRC cases.	C				
2.1	Tracking Requests/Appeals	The system shall assign a tracking number to incoming requests. The system shall allow users to make requests inactive (duplicates or mistakes). Only users with certain privileges shall have the permissions to do so. See 11.1.2	C				
2.2		The system shall be able to identify duplicate requests, requesters' names, subjects' names, companies, and subject matter.	C				
2.3		The system shall assign an appeal number to incoming appeals, and/or shall associate the assigned OIP appeal number for incoming appeals, to the appropriate component's initial FOIA request number.	C				
2.4		The system shall be able to track appeals by both OIP's and the appropriate component's request number, type, requester, and date.	C				

Functional Baseline Requirement

ID	Category	Requirement Description	Priority Code	Vendor Response	Name of Product, Release & Module	LOE to Obtain 100% Fit	Explanation
2.5		The system shall be able to identify duplicate appeals.	C				
2.6		The system shall track multiple parts of an appeal.	C				
2.7		The system shall track DRC appeals by precedent applied and relevant section of the classification/declassification guide.	C				
2.8		The system shall track consultations, referrals, clarification letters, submitter notice letters, fee invoices, etc., and provide notification messages that matters are still awaiting resolution.	C				
2.9		The system shall track whether documents were presented to DRC or whether only a summary was presented to the DRC.	C				
2.10		The system shall track status of each individual document within an initial request (i.e. consultation, concurrence, etc.).	C				
2.11		The system should provide for the tracking of litigation by the components, if desired.	C				
2.12		The system shall allow categorizing requests into types, for example: simple, complex, expedited.	C				
2.13		The system shall track the FOIA Unit's final disposition of each request: (A) full grant; (B) partial grant/partial denial; (C) full denial based on exemptions; (D) no record ; (E) all records referred to another component or agency; (F) request withdrawn; (G) fee-related reason; (H) records not reasonably described; (I) improper FOIA for other reason; (J) not an agency record; (K) duplicate request; (L) other. It shall also allow for customization of disposition codes by the appropriate user.	C				
2.14		The system shall track the final disposition of appeals by OIP: (A) No records; (B) records referred at initial request level; (C) request withdrawn; (D) fee-related reason; (E) records not reasonably described; (F) improper request for other reasons; (G) not agency record; (H) duplicate request or appeal; (I) request in litigation; (J) appeal based solely on denial of request for expedited processing; (K) other. The system shall track the FOIA Unit's final disposition of appeals that were remanded in full or in part to the FOIA Unit for further processing. The system shall track and associate the OIP, FOIA Unit, and civil court case numbers of any resulting FOIA litigation. It shall allow for cutomization of disposition codes by appropriate user.	C				
2.15		The system shall have the ability to track appeals, including appeals completely affirmed, partially affirmed and partially reversed/remanded and completely reversed/remanded.	C				
3.1	**Tracking Fees/Hours**	System shall be able to track fees and any fee waivers granted by the FOIA Staff.	C				
3.1.1.		The system shall track the number of working days it takes to adjudicate a fee waiver. The system shall provide two date entry fields for start and completion dates. The system shall automatically calculate the number of days it took to adjudicate the fee waiver. The system shall track whether the fee waiver was granted or denied.	C				
3.2		System shall be able to track overdue, delinquent accounts and update and generate a report.	C				
3.3		The system shall be able to track time spent on appeals by FOIA staff individually and appeals staff overall.	C				
3.4		The system shall be able to track time spent on requests in 15-minute increments, track when the invoice is sent, and generate a notice to user when fees are due.	D				
3.5		The system shall allow for time sheet type tracking of time spent on requests where a processor can access his or her own time tracking sheet and indicate time spent per case.	D				
3.6		The system shall generate an invoice to the requester with the option for manual adjustment.	D				

Functional Baseline Requirement

ID	Category	Requirement Description	Priority Code	Vendor Response	Name of Product, Release & Module	LOE to Obtain 100% Fit	Explanation
3.7		The system shall distinguish between categories of requesters (commercial use, "other," and media/educational) and categories of FOIA personnel (management, professional, clerical). The system shall be capable of calculating fees according to federal regulations, including amounts charged by categories of FOIA Unit professionals (management: $41/hr, professional: $28/hr, and clerical: $16/hr) and categories of requesters (review and search time plus duplication fees for commercial use requesters; first two hours of search time and first 100 pages of duplication are free of charge for "other" requesters; only duplication charges for media/educational requesters after first 100 free pages; and no charge if fees are less than $14.00). The system shall be capable of easily adjusting the amounts charged as the regulations change, without extensive reprogramming.	D				
		The system shall calculate interest on overdue fees.	D				
4.1	Workflow	The system shall keep track of the deadlines relating to requests such as 20 working days until initial response to requester is due and an extra 10 working days for unusual circumstances. System shall notify appropriate FOIA analyst of the deadline.	C				
4.2		The system shall allow for entry of date received by agency. The system shall also allow for entry of date received by component. The system shall be able to calculate pending days for the request from either receipt by agency date or receipt by component date, depending upon what the user indicates for the particular request. The system shall use the agency date of receipt to start counting the number of days pending when an agency has taken more than ten days to route the request to the proper component. The system shall be able to notify user of deadlines based upon both types of receipt.	C				
4.3		The system shall manage the workflow and track the status where a case requires forwarding portions of a request to other sections of a component, other DOJ components, and/or federal agencies for more information and/or for consultations.	C				
4.4		The system shall allow user to designate a request as perfected or unperfected.	C				
4.5		The system shall allow user to input an estimated date of completion for a request. This shall be in date range format.	D				
4.6		The system shall be able to suspend a case ("stop the clock").	C				
4.7		The system shall keep track of consultations and provide notice to user when response is due. See 2.8.	C				
4.8		The system shall track workflow of requests, status, stages, and indicate next action. See 5.5.	C				
4.9		The system shall track and flag expedited requests and provide notice to user when response to requester is due (10 calendar days, or configurable per component). The system shall track whether request for expedited treatment was granted or denied and shall also allow for tracking of whether an appealed denial of expedited processed was granted or denied.	C				
4.9.1.		The system shall track the number of calendar days it takes to adjudicate a decision to grant or deny expedited review using the date received by a component as the start date. The system shall automatically calculate the number of days it took to adjudicate the request for expedited processing.	C				
4.1		The system shall allow for managing the interaction between OIP and the components in the appeals process as a workflow, if components wish.	C				
4.11		The system shall accommodate various components' workflow requirements	D				
5.1	Reports	The system shall be able to generate and print annual report.	C				
5.2		The system shall be able to generate and print ad-hoc reports.	C				
5.3		The system shall be able to generate backlog reports for both initial requests and appeals that have been pending longer than the statutory time period.	C				

Functional Baseline Requirement

ID	Category	Requirement Description	Priority Code	Vendor Response	Name of Product, Release & Module	LOE to Obtain 100% Fit	Explanation
5.4		Reports will have sortable columns.	D				
5.5		The system shall be able to generate statistical summary reports for each fiscal year, by month, including number of requests on hand at the beginning of each month, number received and closed during month, and number carried over to the next month. The system shall transfer the carry over requests to the next fiscal year. Other reports by fiscal year: annual; backlog; pending; FOIA index; appeals; Privacy Act; dashboard status report for all requests; workload report sorted by FOIA analysts. The dashboard report shall include, type of request (FOIA or Privacy Act), track (simple/ complex/expedite), FOIA analyst's name, request number, date received, date perfected, name of requester and law firm, subject matter of request, case track, fee category of request, fee waiver requested (including granted/denied date), expedited treatment requested (including granted/denied date), type of correspondence (e.g. interim response to requester and date sent), search status, DOJ file number, date files ordered from which sections/Federal Records Center (FRC), date files due from sections/FRC, date files received, date files returned to sections/FRC, date processing completed, date request reviewed, exemptions applied, referral/consultation,	D				
5.6		The system shall allow for reporting and tracking workflow metrics.	D				
6.1	**Balance workload**	The system shall allow for workload monitoring of assignments to FOIA analysts.	C				
6.2		The system shall allow for workload monitoring of assignments to appeals staff.	C				
7.1	**Searching**	The system shall allow for searching of all fields. The system shall provide key word and optical character recognition searching capabilities with optimal accuracy.	C				
7.2		The system shall allow for searching of metadata related to requests and actual content of related documents.	C				
8.1	**Scanning**	The system shall provide the capability to scan documents, with optical character recognition and optimal accuracy, and attach them to requests.	C				
8.2		The system shall be able to provide the option to Bates stamp/number pages of responsive documents with customized page numbers (e.g., ATFY07-065-1).	C				
8.3		The system shall be able to insert and delete pages within responsive documents and renumber the pages, as needed. The system shall allow starting the page numbers with a customized assigned number.	D				
8.4		The system shall scan with optical character recognition and optimal accuracy (99%).	D				
9.1	**Indexing**	The system shall be able to accurately generate separate page counts for the number of pages redacted and various exemptions applied, and the number of pages withheld in entirety and released in entirety.	C				
9.2		The system shall be able to provide the option to Bates Stamp/page number documents, including renumbering pages when pages are inserted into or removed from the documents.	C				
10.1	**Administration**	The system shall provide administrative capabilities and grant administrative rights to add fields, update drop down menus, maintain user roles and permissions.	C				
11.1	**Login and security**	The system shall follow the security requirements.	C				
11.1.1		The system shall only allow authorized users access. All access to component data will be strictly limited to users who are specifically authorized by the respective components. Must also comply with agency password and ID security requirements, See SOW	C				
11.1.2		The system shall require users to enter identification (IDs) and passwords to login.	C				
11.1.3		The system shall recognize authorized user(s), document the identity of the user(s) and track actions taken (audit trail).	C				

Functional Baseline Requirement

ID	Category	Requirement Description	Priority Code	Vendor Response	Name of Product, Release & Module	LOE to Obtain 100% Fit	Explanation
11.1.4		The system shall within specified timeframe automatically require users to change passwords.	C				
11.2	**Create case files**	The system shall allow for creation of a case file once request is received. Case information shall include, type of request (FOIA or Privacy Act); fee category (commercial, other, media/educational); track (simple, complex, expedited); expedited processing requested/granted/denied date; perfected date; date of acknowledgment letter; fiscal year; assigned FOIA control number; component file numbers; date request received; requester name, organization, address, email, phone, fax; subject name or subject matter; assigned FOIA analyst; response type (final, partial, fees, documents sent); response date; amount of fees due; amount of fees paid; date fees paid; number of pages released; number of documents withheld; number of pages withheld; exemption type; exemption statute; type statute; disposition; total days pending; consultation; consultation date; referral; referral date; appealed; OIP appeal number; appeal disposition; appeal comment. Case file will include request letter, all incoming/outgoing correspondence including emails, material responsive to the request, requester's information, all responsive documents (withheld, redacted, and/or released in entirety).	C				
11.2.1		The system shall store cases in a centralized database.	C				
11.2.2		The system shall assign a case number for each new request. The system shall allow users with certain privileges to make requests inactive.	C				
11.2.3		The system shall allow components to customize case number assignments.	C				
11.2.4		The system shall allow for request and supporting documents to be scanned into centralized database.	C				
11.3	**Take action**	Once request is reviewed and a course of action is determined, the system shall allow the analyst to select the action and place case in the appropriate step of the process.	C				
11.3.1		The system shall allow the user to make selection(s) for each step based on his or her analysis of the contents of the incoming request.	C				
11.3.2		The system shall track selection(s) for each step in the process.	C				
11.3.3		The system shall allow users to conduct searches in every field to find duplicate initial requests, for example: by requester's name, subject's name, companies, subject matter, etc.	C				
11.4	**Generate initial response**	The system shall allow the user to generate an initial response to requester.	C				
11.4.1		The system shall generate initial response letter and modified form letters.	C				
11.4.2		The system shall allow the user to select standard letter or input data to customize the letter.	C				
11.4.3		The system shall print acknowledgment letter.	C				
11.4.4		The system shall save acknowledgment letter with the case file.	C				
11.4.5		The system shall keep track of date letter is mailed.	C				
11.4.6		The system shall allow:					
		1. The ability to track decision to grant/deny expedited cases based on calendar days	C				
		2. The ability to track non expedited cases based on working days	C				
		3. The ability to modify working days when necessary (i.e. unscheduled federal holidays)	C				

Functional Baseline Requirement

ID	Category	Requirement Description	Priority Code	Vendor Response	Name of Product, Release & Module	LOE to Obtain 100% Fit	Explanation
11.4.7		The system shall notify analyst about approaching 20-day and 10-day deadlines for responding to initial requests.	C				
11.4.8		The system shall be able to generate electronic responses and notifications to requesters.	D				
11.5	Search for responsive records	The system shall allow for electronic searching of records.	C				
11.5.1		The system shall provide access to components' external systems to search for responsive records.	D				
11.5.2		The system shall allow for identifying duplicate documents.	C				
11.5.3		The system shall be able to distinguish between the final version and drafts of similar documents.	C				
11.6	Request records	The system shall allow the user to generate a modifiable search memorandum to be sent to the appropriate component, section, or field office requesting a search for responsive records.	C				
11.6.1		The system shall generate a modifiable search memorandum to the appropriate component, section, or field office allowing the user to input pertinent information describing responsive records requested.	C				
11.6.2		The system shall allow user to suspend the case ("stop the clock") while waiting for additional information from requester.	C				
11.6.3		The system shall save search memorandum with case file for future access.	C				
11.6.4		The system shall save the date the search memorandum is sent to the responsible office(s) and periodically notify analyst of pending response status.	C				
11.7	Make redactions and apply exemptions	The system shall allow the user to make secure electronic redactions to responsive records. The system shall save the draft with notes, prior to the final redaction of records.	C				
11.7.1		The system shall allow searching and viewing of scanned documents.	C				
11.7.2		The system shall allow secure redaction of the scanned documents with security safeguards that are comparable to industry standard (example: Redax).	C				
11.7.3		The system shall allow the user to apply all FOIA and Privacy Act exemptions on the redacted portion of document and to create customized exemptions including the use of other relevant statutes and text.	C				
11.7.4		The system shall allow the user to make notes on the document being redacted.	C				
11.7.5		The system shall allow highlighting of document, translucent redaction and opaque redaction in various colors.	C				
11.7.6		The system shall allow for page indexing and counting of pages reviewed, exemptions applied, and the option for Bates stamping/page numbering.	C				
11.8	Calculate fees	The system shall be able to calculate fees to be charged to the requester based on time FOIA analyst spends on a request, duplication fees, and the appropriate FOIA regulations. Calculations shall be based on category of reviewer (manager, professional, clerical) and distinguish between review and search time. The system shall provide an option to manually enter recorded time adjustments and to stop and start the clock. Calculations shall be easily adapted, in the event of changes to regulations, without extensive reprogramming.	C				
11.8.1		The system will allow the user to generate a fee invoice and fee letter.	C				
11.8.2		The system shall suspend the request ("stop the clock") when a fee invoice is sent and at the discretion of the user.	C				
11.9	Review redactions	The system shall allow a supervisor or any other predetermined user to review redactions and make changes.	C				
11.9.1		The system shall allow the user to add or delete redactions.	C				

Functional Baseline Requirement

ID	Category	Requirement Description	Priority Code	Vendor Response	Name of Product, Release & Module	LOE to Obtain 100% Fit	Explanation
11.9.2		The system shall allow the user to add or delete exemption codes.	C				
11.9.3		The system shall distinguish between the revisions made by the FOIA analyst, reviewer, and final decision maker by using different colors or another method.	C				
11.9.4		The system shall provide the ability for FOIA analyst, reviewer, and final decision maker to place notes on responsive documents. FOIA analysts shall be able to provide a memo to reviewer/decision maker explaining actions taken in processing request.	C				
11.1	**Generate response**	The system shall allow for a modifiable transmittal letter addressed to the requester to be generated to advise the requester of information pertinent to a partial response or final action, e.g. the amount of information released or withheld, applicable fees, reason for denial of fee waiver.	C				
11.10.1		The system shall allow the user to generate response letter.	C				
11.10.2		The system shall extract pertinent information from FOIA case folder, such as the requester's name and address, and place the data into the appropriate form letter.	C				
11.10.3		The system shall block the printing of notes, e.g., in the final version of the responsive documents to be publicly released, except when appropriate.	C				
11.10.4		The system shall be able to generate electronic responses.	C				
11.11	**Approve release**	The system shall allow a supervisor to review/sign the transmittal letter indicating approval of the redacted responsive records and the calculation of fees.	C				
11.11.1		The system shall allow the user to view redacted image of responsive records, transmittal correspondence, and notes.	C				
11.11.2		The system shall allow the user to enter in a specified data field approval for release.	C				
11.11.3		The system shall track the actions taken.	C				
11.11.4		The system shall save to database the electronic image of the transmittal letter and redacted responsive records for future access.	C				
11.12	**Release records**	The system shall track when the transmittal letter and redacted responsive records are sent to the requester. The system shall allow responsive records to be provided in an electronic format, if desired.	C				
11.12.1		The system shall allow the printing of redacted documents and the final action letter.	C				
11.12.2		The system shall allow for interim releases to be made in a case, and the tracking of those releases.	C				
11.12.3		The system shall allow the printing of selected information at any time.	C				
11.12.4		The system shall be able to provide an electronic copy of redacted documents and the final action letter in the format requested, if available.	C				
11.12.5		The system shall count and store the amount of time required to process the case from receipt to closing (date of the fee invoice/fee letter) for reporting. The system shall be able to stop the clock when, for example, a clarification letter or a fee invoice is sent.	C				
11.12.6		The system shall allow for the closing of a case if case fees are not paid after 30 calendar days, or a configurable number of days (if component's workflow requires that). The system shall notify user when 30 calendar days (or any other configurable number of days) have elapsed, if the fees are delinquent. The amount of days should be configurable per component, based on their business rules. The system shall allow for stopping the clock if fees are delinquent for a determined amount of time. The system shall allow the user to specify the amount of time the clock should be stopped for.	C				
11.12.7		The system shall allow the user to generate fee invoices for requests and generate fee invoices specifically for delinquent fees. The system shall calculate the fees based on predetermined criteria.	C				

Functional Baseline Requirement

ID	Category	Requirement Description	Priority Code	Vendor Response	Name of Product, Release & Module	LOE to Obtain 100% Fit	Explanation
11.13	**Appeals - Prepare case information**	The system shall allow forwarding of a copy of the originating component's initial processing to OIP for review, if the component elects to do so. OIP responds directly to the requester.	C				
11.13.1		The system shall document and save the date appeal is received in FOIA unit and/or OIP. The system shall document and save the date the component's FOIA Unit receives a notice of appeal from OIP.	C				
11.13.2		The system shall provide to the FOIA Unit an electronic image of the appeal letter.	C				
11.13.3		The system shall allow the user to view and print electronic images of all case file documents.	C				
11.13.4		The system shall associate the FOIA request number with OIP's appeal number and provide notice to FOIA Unit of the initial receipt of an appeal and its final disposition (remand, affirm).	C				
11.14	**Appeals - Review OIP decision**	The system shall allow for case reviews and the ability to forward the case and related documents, or notice of the appeal case to appropriate office for re-processing.	C				
11.14.1		The system shall allow the user to remove FOIA exemption codes and reveal original text from the electronic image, possibly by saving a draft with the FOIA exemption codes and that reveals original text in the electronic image, before generating a "burned in" final redacted version.	C				
11.14.2		The system shall allow user(s) to store both the original release and any revisions generated by the appeal.	C				
11.14.3		The system shall allow the FOIA Unit user to print the draft version of the redacted documents. The system shall give the user the option of choosing to print the draft with or without the applied redaction codes and notes showing on the printed pages.	C				
11.15	**Appeals - Generate appeals release**	The system shall allow for the preparation of a remand memo addressing OIP's decision to remand the appeal.	C				
11.15.1		The system shall be able to generate appeals response letter.	C				
11.15.2		The system shall allow for generation of a printed copy of supplemental redacted responsive records.	C				
11.15.3		The system shall allow the component to track status of an appeal.	D				
11.16	**Appeals - Release appeal and Litigation**	The system shall allow for a supplemental release of redacted records.	C				
11.16.1		The system shall track the date the records are mailed to the requester.	C				
11.16.2		The system shall track costs associated with FOIA litigation, including staff time spent on FOIA litigation. The system shall allow for manual input of time recorded.	C				
11.16.3		The system shall track the status and outcome of FOIA litigation.	C				
11.17	**Reports**	The system shall allow for generation of standard, ad-hoc, and annual reports. Statistical reports are requested primarily to satisfy the statutory reporting requirements, as well as internal management needs of the component.	C				
11.17.1		The system shall provide for authorized users to create, select, view, and print reports.	C				
11.17.2		The system shall provide for the display of report on screen after the user makes applicable criteria selections.	C				
11.17.3		The system shall provide for the designated data field elements to be input for reports.	C				
11.17.4		The system shall allow for an ad-hoc reporting function that enables users to generate reports based on a variety of criteria with little or no developer intervention.	C				
11.17.5		The system shall allow the user to print a page header and footer for each report.	D				
11.17.6		The system shall allow the user the flexibility to customize reports without developer assistance.	C				
11.17.7		The system shall allow for reporting and tracking workflow metrics, such as: time a workflow takes, workload, etc.	C				

Functional Baseline Requirement

ID	Category	Requirement Description	Priority Code	Vendor Response	Name of Product, Release & Module	LOE to Obtain 100% Fit	Explanation
11.17.8		The system shall allow annual reports to be created by initial request case type (FOIA, PA, Mandatory Declassification Review, Presidential Records Act) and shall allow certain types of initial requests to be excluded.	C				
11.18	**Reports - Annual**	The system shall be fully compliant with the 2008 Guidelines for Agency Preparation of Annual FOIA Reports issued by the Office of Information and Privacy. The report shall also follow the exact format established in the Guidance. The system shall allow for generation of an annual report by fiscal year, using the data maintained by the system, containing the following requirements:	C				
11.18.1		List of Exemption 3 statutes relied upon.	C				
11.18.2		Description of the type of information withheld under each Exemption 3 statute.	C				
11.18.3		Citation of court case upholding each Exemption 3 statute.	C				
11.18.4		Total number of times each Exemption 3 statute was used.	C				
11.18.5		Number of initial FOIA requests pending as of the start of fiscal year.	C				
11.18.6		Number of initial FOIA requests received in fiscal year.	C				
11.18.7		Number of initial FOIArequests processed in fiscal year.	C				
11.18.8		Number of initial FOIA requests pending as of end of fiscal year.	C				
11.18.9		Disposition of initial FOIA requests: Number of requests granted in full. Number of partial grants/ partial denials. Number of full denials based on exemptions.	C				
11.18.10		Number of Full Denials Based on Reasons Other Than Exemptions a. No records b. All records referred to another component or agency c. Request withdrawn d. Fee-related reason e. Records not reasonably described f. Improper FOIA request for other reason g. Not an agency record h. Duplicate request i. Other (shall allow for component to add additional reasons for denial which shall be counted for each "other" disposition and also counted as a total "other")	C				

Functional Baseline Requirement

ID	Category	Requirement Description	Priority Code	Vendor Response	Name of Product, Release & Module	LOE to Obtain 100% Fit	Explanation
11.18.11		Disposition of FOIA Requests Number of times each FOIA exemption was applied: Exemption 1 Exemption 2 Exemption 3 Exemption 4 Exemption 5 Exemption 6 Exemption 7(A) Exemption 7(B) Exemption 7(C) Exemption 7(D) Exemption 7(E) Exemption 7(F) Exemption 8 Exemption 9	C				
11.18.12		Number of appeals pending as of the start of fiscal year.	C				
11.18.13		Number of appeals received in fiscal year.	C				
11.18.14		Number of appeals processed in fiscal year.	C				
11.18.15		Number of appeals pending as of end of fiscal year.	C				
11.18.16		Disposition of appeals: Number of appeals completely affirmed Number of appeals partially affirmed and partially reversed/remanded Number of appeals completely reversed/remanded Number of Appeals Closed for Other Reasons	C				
11.18.17		Reasons for Denial on Appeal - Number of times exemptions applied (counting each exemption once per appeal) Exemption 1 Exemption 2 Exemption 3 Exemption 4 Exemption 5 Exemption 6 Exemption 7(A) Exemption 7(B) Exemption 7(C) Exemption 7(D) Exemption 7(E) Exemption 7(F) Exemption 8 Exemption 9	C				
11.18.18		Reasons for Denial on Appeal - Reasons Other than Exemptions 1. No records 2. Records referred at initial request level 3. Request withdrawn 4. Fee-related reason 5. Records not reasonably described 6. Not a proper request for other reasons 7. Not agency record 8. Duplicate request or appeal 9. Request in litigation 10. Appeal based solely on denial of expedited processing 11. Other (shall allow for entry of additional reasons for denial which shall be counted for each "other" disposition and also counted as a total "other")	C				
11.18.19		Response time for all appeals 1. Median number of days to respond 2. Average number of days to respond 3. Lowest number of days to respond 4. Highest number of days to respond	C				
11.18.20		The date of receipt for each of the ten oldest appeals	C				
11.18.21		Number of days pending for each of the ten oldest appeals	C				

Functional Baseline Requirement

ID	Category	Requirement Description	Priority Code	Vendor Response	Name of Product, Release & Module	LOE to Obtain 100% Fit	Explanation
11.18.22		Initial FOIA Requests (Perfected requests only) Response time for processed requests: median, average and range of time to process all requests. 1. Simple request (if multiple tracks used) a. Median number of days to process b. Average number of days to process c. Lowest number of days to process d. Highest number of days to process 2. Complex requests (specify for any and all tracks used) a. Median number of days to process b. Average number of days to process c. Lowest number of days to process d. Highest number of days to process 3. Requests accorded expedited processing a. Median number of days to process b. Average number of days to process c. Lowest number of days to process d. Highest number of days to process	C				
11.18.23		Initial FOIA Requests (Perfected requests only) Response time for processed requests: median, average and range of time to process requests in which information was granted (includes requests that had a full grant and partial grant): 1. Simple request (if multiple tracks used) a. Median number of days to process b. Average number of days to process c. Lowest number of days to process d. Highest number of days to process 2. Complex requests (specify for any and all tracks used) a. Median number of days to process b. Average number of days to process c. Lowest number of days to process d. Highest number of days to process 3. Requests accorded expedited processing a. Median number of days to process b. Average number of days to process c. Lowest number of days to process d. Highest number of days to process	C				
11.18.24		The date of receipt for each of the ten oldest FOIA requests (perfected)	C				
11.18.25		Number of days each of the ten oldest FOIA requests have been pending	C				

Functional Baseline Requirement

ID	Category	Requirement Description	Priority Code	Vendor Response	Name of Product, Release & Module	LOE to Obtain 100% Fit	Explanation
11.18.26		Initial FOIA Requests Response time for processed requests: Number of requests processed in day increments 1. Simple requests (if multiple tracks used) 1 – 20 days 21 – 40 days 41 – 60 days 61 – 80 days 81 – 100 days 101 – 120 days 121 – 140 days 141 – 160 days 161 – 180 days 181 – 200 days 201 – 300 days 301 – 400 days 401 or more days 2. Complex requests (specify for any and all tracks used) 1 – 20 days 21 – 40 days 41 – 60 days 61 – 80 days 81 – 100 days 101 – 120 days 121 – 140 days 141 – 160 days 161 – 180 days 181 – 200 days 201 – 300 days 301 – 400 days 401 or more days 3. Requests accorded expedited processing 1 – 20 days 21 – 40 days 41 – 60 days 61 – 80 days 81 – 100 days 101 – 120 days 121 – 140 days 141 – 160 days 161 – 180 days 181 – 200 days 201 – 300 days 301 – 400 days 401 or more days	C				
11.18.27		All Pending Perfected Requests Pending requests: number of perfected requests pending, median, and average number of days pending 1. Simple request (if multiple tracks used) a. Number Pending b. Median number of days c. Average number of days 2. Complex requests (specify for any and all tracks used) a. Number Pending b. Median number of days c. Average number of days 3. Requests accorded expedited processing a. Number Pending b. Median number of days c. Average number of days	C				

Functional Baseline Requirement

ID	Category	Requirement Description	Priority Code	Vendor Response	Name of Product, Release & Module	LOE to Obtain 100% Fit	Explanation
11.18.28		Requests for expedited processing (includes appeals): 1. Number granted 2. Number denied 3. Median number of days to adjudicate whether to grant or deny expedited review (in calendar days) 4. Average number of days to adjudicate whether to grant or deny expedited review (in calendar days) 5. Number of FOIA requests for expedited review that are adjudicated (granted or denied) within ten calendar days	C				
11.18.29		Requests for fee waiver: 1. Number granted fee waiver 2. Number denied fee waiver 3. Median number of days to adjudicate whether to grant or deny fee waiver (in working days) 4. Average number of days to adjudicate whether to grant or deny fee waiver (in working days)	C				
11.18.30		A. Staffing levels System shall be able to calculate the number of "equivalent full-time FOIA employees" in accordance with Section IX of the OIP 2008 Guidance for Annual Reports 1. Number of full-time FOIA employees 2. Number of "Equivalent Full-time FOIA Employees" 3. Total number of "Full-Time FOIA Staff" B. Costs 1. Processing (including appeals) 2. Litigation-related costs 3. Total costs	C				
11.18.31		Total amount of fees collected for processing requests and what percentage this is of the total FOIA processing costs.	C				
11.18.32		Number of backlogged (initial) requests as of the end of the fiscal year	C				
11.18.33		Number of backlogged appeals as of the end of the fiscal year	C				
11.18.34		Number of consultations received from other agencies that were pending at the start of the fiscal year. (System shall be able to distinguish a consult from a component within the Department and one from other agency.)	C				
11.18.35		Number of consultations received from other agencies during the fiscal year	C				
11.18.36		Number of consultations received from other agencies that were processed in fiscal year	C				
11.18.37		Number of consultations received from other agencies that were pending as of end of fiscal year	C				
11.18.38		The date of receipt for each of the ten oldest consultations received from other agencies and the number of days pending	C				
11.18.39		Number of (Initial) Requests Received Number received during fiscal year from last year's annual report. Number received during fiscal year from current annual report.	C				

Functional Baseline Requirement

ID	Category	Requirement Description	Priority Code	Vendor Response	Name of Product, Release & Module	LOE to Obtain 100% Fit	Explanation
11.18.40		Number of Requests Processed Number processed during fiscal year from last year's annual report. Number processed during fiscal year from current annual report.	C				
11.18.41		Number of backlogged requests as of end of the fiscal year from last year's annual report. Number of backlogged requests as of the of the fiscal year from current annual report.	C				
11.18.42		Number of Appeals Received Number received during fiscal year from last year's annual report. Number received during fiscal year from current annual report.	C				
11.18.43		Number of Appeals Processed Number processed during fiscal year from last year's annual report. Number processed during fiscal year from current annual report.	C				
11.18.44		Number of backlogged appeals as of the end of the fiscal year from previous annual report.	C				
11.18.45		Number of backlogged appeals as of end of the fiscal year from current annual report.	C				
11.18.46		The system shall be able to create annual reports at both the component level and at the agency level. At the component level, the system shall automatically generate the report based upon data already entered in the system. At the agency level, the system shall be able to automatically transfer component data from components that are using the system to the agency annual report. The system shall also allow for the manual input of component-level data into the agency annual report. Vendor shall also propose a solution that would allow for the automatic transfer of components' annual report data, for components not using the system, which would be used in the creation of the agency annual report.	C				
11.18.47		Vendor shall propose a solution that would allow for the calculation of agency-wide medians and averages by using raw data of components, taking into account that not all components will be on the system.	C				
11.18.48		Vendor shall propose a solution that would allow for component-level and agency raw data to be saved in an electronic format which can be made available to the public upon request.	C				
11.19	**Maintain files**	The system shall allow for the electronic retention of case files for 6 years (or time determined by the FOIA Units in the different components) and then files will be archived by system.	C				
11.20	**Reading rooms**	The system shall allow for publishing of information to a web site in compliance with Sec. 508 of the Rehabilitation Act.	C				

Technical Baseline Requirement

ID	Category	Requirement Description	Priority Code	Vendor Response	Name of Product, Release & Module	LOE to Obtain 100% Fit	Explanation
SE1	**Security**	If the system is a browser-based application, the system shall provide a solution that does not require the use of persistent cookies on a user's machine.	C				
SE2		System shall operate in an environment that incorporates firewalls, providing only authorized users access to the system.	C				
SE3		The system shall support the ability to define an "inactivity time-out" period.	C				
SE4		The system shall protect and secure user logons and passwords from unauthorized access.	C				
SE5		The system shall support multiple levels of security access to information and system functionality based on user and user group profiles.	C				
SE6		The system shall require authentication of all user IDs and passwords before allowing access to the system.	C				
SE7		The system shall provide the ability to define user profiles and establish groups of users with like attributes and system rights. (i.e., changes to the group automatically apply to each individual user of that group).	C				
SE8		The system shall be able to create user logons and passwords.	C				
SE9		System will track the following information for all events/activities within a history of occurrences: user ID, date and time of access, date and time of terminated access, type of event (ex: insert, update, delete), data or transaction change.	C				
SE10		The system shall support viewing, searching, and reporting on audit trails based on user-defined parameters.	C				
SE11		All system audit trail information will be available for a user-defined period then archived for a user-defined period, or the period specified in the system security plan.	C				
SE12		If the system is a browser-based application, the system shall log off a user when browser window is closed.	C				
SE13		If the system is a browser-based application, the system shall close all browser windows when a user logs off.	C				
SE14		The system shall provide multiple layers of access and data protection based on the user's ID/password, role, and office assignment. The user role defines the type of access (update, insert, delete, read only).	C				
SE15		The system shall have the ability to encrypt sensitive data, such as passwords, employee/contractor personal information and SSNs in the database.	C				
SE16		For Certification and Accreditation purposes the system shall meet the security requirements as specified on Section 2.9.9 of the BPA.	C				
RE1	**Reliability**	The system shall not exceed one (1) hour of unplanned downtime due to a system failure over a 30-day period.	D				
RE2		The system shall provide automated notifications regarding system unavailability, database errors, communication errors, or other system exception.	D				

Technical Baseline Requirement

ID	Category	Requirement Description	Priority Code	Vendor Response	Name of Product, Release & Module	LOE to Obtain 100% Fit	Explanation
RE3		In the event of database corruption or destruction, the database must be capable of being restored from backup.	C				
RE4		A stand-by server (automatic failover) shall be included in the application architecture.	D				
RE5		A disaster recovery server shall be included in the application architecture.	D				
RE6		The system shall be able to create "hot" backups that do not require system downtime.	D				
RE7		The system shall be capable of being operational 24 hours a day, 7 days a week.	D				
RE8		The system shall be capable of functioning within an environment that uses Instrumentation Monitoring Software.	D				
DA1	**Data Requirements**	The system information must be retained in an immediately accessible format for six (6) years from the closing date of non-litigation records, and ten (10) years from the closing date of litigation records. The system shall allow for manual overriding of the data retention rules. The system shall prompt for purging rather than purge automatically, and allow users to override.	C				
DA2		The system shall provide archival capabilities of all electronic records including electronic images, supporting documents, and system data.	C				
DA3		All data requests for viewing, reporting, inserting, and updating within the system database shall be real-time.	C				
DA4		The system shall provide the ability for authorized system users to arrange the data elements in categories in order to facilitate logical dataset groupings and data input screens.	D				
DA5		The system shall record the source of data inputs within an audit trail.	C				
DA6		The system shall provide the ability to create new data elements and group data elements into datasets.	D				
SU1	**Supportability**	The system shall be capable of operating with multiple databases using industry standard connectivity methods (e.g., ODBC, JDBC).	C				
SU2		The system shall support a modular approach that enables components of the system to be managed independently.	D				
SU3		The system shall have a documented data model.	D				
SU4		The system shall have a documented application programming interface (API).	D				
PE1	**Performance**	The system shall be able to process and store data pertaining to approximately 100 simultaneous users, 5,000 transactions per month with an estimated 50% annual growth rate. The monthly transactions are based on interactive data entry, reports responses and batch data entry. This is system-generated data.	D				

Technical Baseline Requirement

ID	Category	Requirement Description	Priority Code	Vendor Response	Name of Product, Release & Module	LOE to Obtain 100% Fit	Explanation
PE2		System architecture shall support the following response times: Less than 2 seconds for returning results of transaction processing, immediate response when tabbing from field to field, less than 2 seconds when moving from screen to screen, immediate to retrieve a single record.	C				
PE3		Initially, the system shall be able to support approximately 100 users in multiple geographic locations (average of 30 concurrent users, 50 concurrent users during peak times).The number of users for subsequent phases of component implementation will be determined at the time of requirements gathering for each component implementation.	C				

System Deployment and Support

ID	Requirement Description	Priority Code	Vendor Response	Degree of Fit	Name of Product, Release & Module	LOE to Obtain 100% Fit	Explanation
System Deployment and Support							
SDS-1	The vendor should provide and maintain an Entity Relationship Diagram (ERD).	D					
SDS-2	The vendor shall provide separate instances to process classified and unclassified data.	D					
SDS-3	The vendor shall provide and use a common, integrated fully attributed data dictionary that allows for the documentation of the specific use of fields and values.	C					
SDS-4	The system shall be compatible with automated software distribution tools, e.g., web or Marimba-distributable client, to support new installations and upgrades.	C					
SDS-5	The vendor shall provide multi-tiered user support consisting of service-level agreements and clearly defined issue escalation and resolution procedures.	C					
SDS-6	The vendor shall provide user software manuals and release notes in electronic format, available on-line or in CD-ROM format.	C					
SDS-7	The vendor shall provide an e-mail address where client users can submit questions, issues or comments over the Internet.	C					
SDS-8	The vendor shall provide an initial response to a client user within 4 hours of contact. Questions that cannot be resolved immediately shall be escalated to the appropriate organization for disposition.	D					
SDS-9	The vendor shall provide a knowledge database, available through the internet, of all incident reports, their status, and their resolution.	D					
SDS-10	The vendor shall publish a technical and functional notice alerting users of issues prior to the implementation of new releases or patches.	D					
SDS-11	The vendor shall provide a domestic toll free number and an international number to assist client users with questions related to product operation. The support staff is available 9am-5:30pm.	D					
SDS-12	The vendor shall support standard licensing for concurrent user or individual seat licensing, or a hybrid of the two.	C					

ID	Requirement Description	Priority Code	Vendor Response	Degree of Fit	Name of Product, Release & Module	LOE to Obtain 100% Fit	Explanation
SDS-13	Reserved	D					
SDS-14	The vendor shall provide different licensing models depending upon user functionality or deployment architecture.	D					
SDS-15	The vendor shall provide a flexible warranty and maintenance schedule that can be tailored to the agencies needs.	C					
SDS-16	The vendor shall provide maintenance for any vendor customization to the core software.	C					
SDS-17	The vendor shall provide routine maintenance for system updates required as a result of statutory, regulatory, and/or policy changes.	C					
SDS-18	The vendor shall provide a warranty for any vendor customization to the core software.	C					
SDS-19	The vendor shall provide training for end users and system administrators via instructor led training and a variety of media to include computer-based training (CBT), web based, or other virtual training.	D					
SDS-20	The vendor shall provide training materials which have been tailored for the specific configuration of the FOIA solution.	C					
SDS-21	The vendor should provide procedural related training that has been tailored to the specific configuration of the delivered FOIA solution.	D					
SDS-22	The vendor shall provide "Train the Trainer" methodologies to assist in training deployment.	D					
SDS-23	The vendor shall provide web based training administration to monitor end-user and system administrator training status.	D					
SDS-24	The system shall be able to integrate with existing Oracle databases that host human resource, matter tracking, and time reporting systems.	D					
SDS-25	The system shall support development/test and production environments, as described in the "SDS Development Environment Infrastructure" and the "Production Hosting High Level Design" attachements.	C					
SDS-26	Vendor should configure desktops and environments to best accommodate the system.	C					
SDS-27	System shall be compatible with the different technical standards (such as Desktop Operating systems and browsers)	C					