AWARD/CONTRACT

1. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 350)

Rating

Page 1 of Pages 4

2. CONTRACT *(Proc. inst. ident.)* NO.
DOC50PAPT401015

3. EFFECTIVE DATE
03/31/2004

4. REQUISITION/PURCHASE REQUEST PROJECT NO.
293P0430199

5. ISSUED BY CODE *

OFFICE OF PROCUREMENT
Office of Procurement
US Patent and Trademark Office
2011 Crystal Drive Suite 810

Arlington, VA 22202

6. ADMINISTERED BY *(If other than Item 5)* CODE 000PA

Office of Procurement -
U.S. Patent and Trademark Office
2011 Crystal Drive, Suite 810

Arlington, VA 22202

7. NAME AND ADDRESS OF CONTRACTOR *(No., street, city, county, State and ZIP Code)*

Electronic Consulting Services
1801 Reston Parkway
Suite 100
Reston, VA 20190-3389

CODE *

FACILITY CODE 000PA

8. DELIVERY □ FOB Origin ☑ Other (See below)

9. DISCOUNT FOR PROMPT PAYMENT

10 days	%
20 days	%
30 days	%
days	%

10. SUBMIT INVOICES *(4 Copies unless other - - wise specified)* TO THE ADDRESS SHOWN IN:

ITEM 12

11. SHIP TO/MARK FOR CODE
No Contacts Identified

12. PAYMENT WILL BE MADE BY CODE *

Office of Finance -
U.S. Patent & Trademark Office
2011 Crystal Drive, Suite 802

Arlington, VA 22202-

13. AUTHORITY FOR USING OTHER THAN FULL AND OPEN COMPETITION:

□ 10 U.S.C. 2304(c) ( ) □ 41 U.S.C. 253(c) ( )

14. ACCOUNTING AND APPROPRIATION DATA
See Funding Detail

15A. ITEM NO.	15B. SUPPLIES/SERVICES	15C. QUANTITY	15D. UNIT	15E. UNIT PRICE	15F. AMOUNT
	SEE LINE ITEM DETAIL				

15G. TOTAL AMOUNT OF CONTRACT 537,120.00

16. TABLE OF CONTENTS

CONTRACTING OFFICER WILL COMPLETE ITEM 17 OR 18 AS APPLICABLE

17. ☑ CONTRACTOR'S NEGOTIATED AGREEMENT *(Contractor is required to sign this document and return* 3 *copies to issuing office)* Contractor agrees to furnish and deliver all items or perform all the services set forth or otherwise identified above and on any continuation sheets for the consideration stated herein. The rights and obligations of the parties to this contract shall be subject to and governed by the following documents: (a) this award/contract, (b) the solicitation, if any, and (c) such provisions, representations, certifications, and specifications, as attached or incorporated by reference herein.

(Attachments are listed herein.)

18. □ AWARD *(Contractor is not required to sign this document.)* Your offer on Solicitation Number ____________________ including the additions or changes made by you which additions or changes are set forth in full above, is hereby accepted as to the items listed above and on any continuation sheets. This award consummates the contract which consists of the following documents: (a) the Government's solicitation and your offer, and (b) this award/contract. No further contractual document is necessary.

19A. NAME AND TITLE OF SIGNER *(Type or print)*

20A. NAME OF CONTRACTING OFFICER
Brenda L. Carswell

19B. NAME OF CONTRACTOR
By ____________________
(Signature of person authorized to sign)

19C. DATE SIGNED

20B. UNITED STATES OF AMERICA
By ____________________
(Signature of Contracting Officer)

20C. DATE SIGNED

Line Item Summary	Document Number	Title	Page
	DOC50PAPT401015	Data Quality and Records Management	2 of 4

Total Funding: $537,120.00

FYs	Fund	Budget Org	Sub	Object Class	Sub	Program	Cost Org	Sub	Proj/Job No.	Sub	Reporting Category
See Line Item(s)											

Division	Closed FYs	Cancelled Fund

Line Item Number	Description	CLIN Ref	Delivery Date (Start Date to End Date)	Quantity	Unit of Issue	Unit Price	Total Cost (Includes Discounts)
0001		0000	05/01/2004 (05/01/2004 to 09/30/2004)			$.000	

Ref Req No: 293P0430199

Total Cost: $0.00

2004 - - A - 293100 - - 2570 - - C50041 - 293410 - - - - NONCOMP - - - -

$21,200.00

Reference Requisition: 293P0430199

2004 - - A - 293100 - - 2570 - - P50041 - 293410 - - - - NONCOMP - - - -

$179,130.00

Reference Requisition: 293P0430199

2004 - - A - 293100 - - 2570 - - P50045 - 293410 - - - - NONCOMP - - - -

$119,200.00

Reference Requisition: 293P0430199

2004 - - A - 293100 - - 2570 - - T50045 - 293410 - - - - NONCOMP - - - -

59,600.00

Reference Requisition: 293P0430199

2004 - - A - 293100 - - 2570 - - L50045 - 293410 - - - - NONCOMP - - - -

$14,900.00

Reference Requisition: 293P0430199

2004 - - A - 293100 - - 2570 - - D50045 - 293410 - - - - NONCOMP - - - -

$59,600.00

Reference Requisition: 293P0430199

2004 - - A - 293100 - - 2570 - - MZTSC1 - 293410 - - - - NONCOMP - - - -

$57,140.00

Reference Requisition: 293P0430199

2004 - - A - 293100 - - 2570 - - MZTSC1 - 293410 - - - - NONCOMP - - - -

$26,350.00

Reference Requisition: 293P0430199

Total Funding: $537,120.00

TABLE OF CONTENTS

SECTION I -- CONTRACT CLAUSES

SECTION B -- SUPPLIES OR SERVICES AND PRICES

B.1 SCHEDULE OF ITEMS AND PRICES - LABOR HOUR

BASE YEAR

4/1/04 - 3/30/2005

LABOR CATEGORY	**TOTAL HOURS**	**PRICE PER HOUR**
Technical Program/Project Manager	500 staff hours	$115.00
Senior Data Quality Management Specialist	2000 staff hours	$164.23
Junior Data Quality Management Specialist	2000 staff hours	$87.98
Senior Records Management Specialist (1)	4000 staff hours	$84.96
Senior Records Management Specialist (2)	4000 staff hours	$75.54
Two Junior Records Management Specialists	4000 staff hours	$59.53
Technical Writer/Editor	1000 staff hours	$45.00
TOTAL	13,500 staff hours	

OPTION YEAR 1

April 1, 2005 - March 30, 2001

LABOR CATEGORY	**TOTAL HOURS**	**PRICE PER HOUR**
Technical Program/Project Manager	500 staff hours	$118.45
Senior Data Quality Management Specialist	2000 staff hours	$169.16
Junior Data Quality Management Specialist	2000 staff hours	$90.62
Senior Records Management Specialist (1)	4000 staff hours	$87.51
Senior Records Management Specialist (2)	4000 staff hours	$77.81
Two Junior Records Management Specialists	4000 staff hours	$61.32
Technical Writer/Editor	1000 staff hours	$46.35
TOTAL	13,500 staff hours	

OPTION YEAR 2

LABOR CATEGORY	**TOTAL HOURS**	**PRICE PER HOUR**
Technical Program/Project Manager	500 staff hours	$122.00
Senior Data Quality Management Specialist	2000 staff hours	$174.23
Junior Data Quality Management Specialist	2000 staff hours	$93.34
Senior Records Management Specialist (1)	4000 staff hours	$90.14
Senior Records Management Specialist (2)	4000 staff hours	$80.14
Two Junior Records Management Specialists	4000 staff hours	$63.16
Technical Writer/Editor	1000 staff hours	$47.74
TOTAL	13,500 staff hours	

Apr. 1, 2006 -
March 30, 2007

OPTION YEAR 3

LABOR CATEGORY	**TOTAL HOURS**	**PRICE PER HOUR**
Technical Program/Project Manager	500 staff hours	$125.66
Senior Data Quality Management Specialist	2000 staff hours	$179.46
Junior Data Quality Management Specialist	2000 staff hours	$96.14
Senior Records Management Specialist (1)	4000 staff hours	$92.84
Senior Records Management Specialist (2)	4000 staff hours	$82.54
Two Junior Records Management Specialists	4000 staff hours	$65.05
Technical Writer/Editor	1000 staff hours	$49.17
TOTAL	13,500 staff hours	

April 1, 2007
March 30, 2008

OPTION YEAR 4

LABOR CATEGORY	TOTAL HOURS	PRICE PER HOUR
Technical Program/Project Manager	500 staff hours	$129.43
Senior Data Quality Management Specialist	2000 staff hours	$184.84
Junior Data Quality Management Specialist	2000 staff hours	$99.02
Senior Records Management Specialist (1)	4000 staff hours	$95.63
Senior Records Management Specialist (2)	4000 staff hours	$85.02
Two Junior Records Management Specialists	4000 staff hours	$67.00
Technical Writer/Editor	1000 staff hours	$50.65
TOTAL	13,500 staff hours	

April 1, 2008
March 30, 2009

SUMMARY ALL YEARS

LABOR CATEGORY	TOTAL HOURS
Technical Program/Project Manager	2,500 staff hours
Senior Data Quality Management Specialist	10,000 staff hours
Junior Data Quality Management Specialist	10,000 staff hours
Senior Records Management Specialist (1)	10,000 staff hours
Senior Records Management Specialist (2)	10,000 staff hours
Two Junior Records Management Specialists	20,000 staff hours
Technical Writer/Editor	5,000 staff hours
TOTAL	67,500 staff hours

B.2 CEILING PRICE

The ceiling price for this contract is $5,414,180 for the five year period of performance.

B.3 BURDENED RATES

ſhe prices set forth in Section B.1 shall be inclusive of all labor and material costs, burdens, any other direct costs, and profit.

B.4 TASK ORDER PROCEDURES

All work shall be initiated only by issuance of a task order fully executed by the CO. The Government is only liable for Labor hours expended under the terms and conditions of this contract to the extent that a fully executed task order has been issued and covers the required work. Charges for any work not authorized will be disallowed.

The designated COTR will initiate the task order process by preparing a statement of requirements and/or objectives to be achieved which includes performance measures in the form of a Task Objective Statement (TOS). The Contractor shall meet with the COTR to mutually discuss and agree upon the requirements and/or objectives to be achieved.

The Contractor shall prepare a proposal in response to the TOS incorporating the results of the discussions and forward it to the COTR for approval. The proposal shall contain the effective date of the task order, and the COTR and designated Task Manager's names as delineated in the TOS, a detailed description of the functional or other objectives to be achieved, a schedule for completion of the task order, any deliverables to be provided by the task order, any Government-furnished equipment, any Contractor-furnished items required, the labor categories required, the anticipated level of effort, and a cost ceiling.

Jpon approval of the proposal by the COTR the final task order statement of work will be forwarded to the CO for execution and issuance.

The Contractor shall acknowledge receipt of each task order by returning to the CO a signed copy of the task order within two (2) work days after receipt. The Contractor shall begin work on the task order in accordance with the effective date indicated on the task order.

Following execution of the task order, technical clarifications may be issued in writing at any time by the designated COTR to amplify or provide additional guidance to the Contractor regarding performance of the task order. The Contractor shall notify the CO of any instructions or guidance the Contractor considers to be a change to the task order which will impact the cost, schedule or deliverables content of the baseline work plan. In cases where technical instructions or other events may dictate a change from the baseline, task orders may be formally modified in writing by the CO to reflect changes to tasking.

The Contractor shall not exceed the ceiling price established in each Task Order. If at any time the Contractor has reason to believe that the total amount for the Task Order, will exceed 80% (percent) of the ceiling price specified in the order, the Contractor shall notify the CO. Such notification shall include an estimate of the additional amount and, if necessary, additional time required for completion of the ordered work.

Task orders may be placed during the period of performance of the contract. Labor rates applicable to hours expended in performance of an order will be the contract rates that are in effect at the time the task order is executed. Any order issued during the period of performance of this contract and not completed within that time shall be governed by the contract terms to the same extent as if the order were completed during the contract's period of performance, including the contract and individual order ceiling prices. Work performed on such orders after the end of the contract's period of performance shall continue to be charged at the last effective rates.

SECTION C - DESCRIPTION/SPECIFICATIONS/WORK STATEMENT

C.1 STATEMENT OF WORK/SPECIFICATIONS

The contractor shall furnish the necessary personnel, material, equipment, cell phones, pagers, services, and facilities (except as otherwise specified), in performance of the following Statement of Work/Specifications.

C.1.1 BACKGROUND

USPTO-wide data quality management of its automated systems' activities is aimed at providing clear, concise, consistent and unambiguous business data throughout the USPTO and in applications shared throughout the worldwide intellectual property community. The program addresses such data requirements as accuracy, and improves management decision making through more accurate data.

Records management is a USPTO-wide function that ensures compliance with federal laws and regulations and helps business areas operate more efficiently though the use of optimum records management practices. Effective controls are created over the maintenance and use of automated and paper records that are used to conduct current business Standards. Procedures and techniques are introduced and instituted to improve the management of records; to promote the maintenance and security of records that must be preserved; and to facilitate records disposition and access.

The USPTO is operating under a Congressional mandate to implement state-of-the-art computer data and information retrieval systems in support of virtually all aspects of its operations.

C.1.2 PURPOSE

The role of the Data Quality Management and Records Management contractor shall be to support the USPTO in its agency-wide records management function in order to comply with the Congressional mandate as an independent and objective source.

C.2 SCOPE OF CONTRACT

The contractor shall perform independent enhancement of existing automated information systems (AIS) by designing and implementing changes to the data systems infrastructure, to support data quality and records management initiatives, that will provide support to the patent and trademark application processing and examination functions, USPTO management and administrative systems, and dissemination of patent and trademark information to the public through the year 2003 and beyond. This is done through assessment review of the current AISs' data bases, generating reports that show the data anomalies, and correcting data errors based on user's approval.

The contractor shall perform administrative and technical support for records management and information collection activities. They shall manage federal information resources.

Subsections C.3.1 discuss Data Quality Management and 3.2 the Records Management areas in more details.

C.2.1 ORDERING

The USPTO's Contracting Officer will order services by the unilateral issuance of a written task order for each specific task to be performed by the Contractor . Section B.3 TASK ORDER PROCEDURES of the contract details for the ordering procedures.

C.3 SCOPE OF WORK TO BE PERFORMED UNDER THE CONTRACT

C.3.1 DATA QUALITY MANAGEMENT

BACKGROUND

The USPTO has established a data quality guidelines document on how to measure accuracy and completeness in the data bases (Attachment 1). The Contractor shall be required to perform data quality in accordance with these guidelines. The data quality is a component of the USPTO's strong data management program. Additional components of the data management program include enterprise data architecture, which is comprised of enterprise data modeling, data element standardization, and enterprise information repository, data stewardship, and SGML/XML Resources Repository.

The data quality program has been applied OCIO-wide since March 1996. Its purpose is to measure the USPTO's ability to convert data into mission-critical information and correct any problems, such as compliance to business rules that govern data. The data quality program strives to enforce a data quality management process that systematically conducts audits, sets up monitoring systems and certifies business critical data. The USPTO anticipates that implementing the data quality activities will lower the costs of automated support to the USPTO community and streamline the exchange of technical and management information.

The data quality program was launched in 1996 as a pilot. The data quality management staff, working with data users and creators, conducted assessments and cleanup of data in existing Automated Information Systems, targeting Patent Application Location and Monitoring System Replacement and Trademark Reporting and Monitoring System Replacement and data conversion efforts. After defining lessons learned from the assessments of these automated systems, the USPTO expanded activities of the data quality program to cleanup customer address data, implement Data Quality Management guidelines – Attachment 7, and use data quality analysis tools USPTO-wide.

The data quality management staff conducted assessments and clean up of data in existing Automated Information Systems over the last several years. The new automated information systems that USPTO designed with proven high quality data receive better feedback from users when the system is delivered. Delivering and maintaining quality data support major USPTO goals. These goals are defined and approved in the USPTO Data Management Policy of data sharing, interoperability, and reuse.

C.3.1.1 SCOPE OF WORK – DATA QUALITY MANAGEMENT

The systems for Data Quality Management, covered under this contract currently utilize Oracle. The contractor must be knowledgeable about various database management systems (DBMSs), especially: Oracle 7 through Oracle 9.n, Access, Microsoft SQL, SQL*NET, DB2. Also, knowledge of using ODBC driver to connect to external databases from both the Quality Manager and dfPower Studio tools.

The contractor is required to provide data quality management support by performing the following activities. Activities will include but are not limited to:

- performing data quality assessments for databases in legacy and development Patent, Trademark, Dissemination, and Corporate automated information systems;
- establishing and refining data quality assessment techniques;
- performing data cleansing in Patent, Trademark, Dissemination, and Corporate data bases;
- verifying data transformation;
- ensuring data conforms to business rules that is processed in the aforementioned systems; and
- database certification with the OCIO development teams and business users.

The contractor shall 1) assess USPTO data in the Patent, Trademark, Dissemination, and Corporate automated information systems using data quality tools such as Ascential Software's Quality Manager and DataFlux's dfPower Studio; 2) provide data quality tool training; and 3) perform data quality management strategic planning.

The contractor shall perform all data analysis in accordance with USPTO Life Cycle Management (LCM) policies – Attachment 10, security policies, Information Technology policies and procedures, data quality management standards and guidelines including, but not limited to:

a) Data Management Technical Standard and Guideline (TSG) – Attachment 9

b) Data Element Naming Conventions and Standardization TSG – Attachment 8

c) Electronic Records Management

d) Standard Generalized Markup Language /eXtensible Markup Language /Resource Management Guidelines – Attachment 3

Data Quality activities support the E-Government 1 & 2 Action Plans (Trademark & Patent E-Government) (see http://www.uspto.gov/web/offices/com/strat21/index.htm, Strategic Plan, page 8). The practical aspect of data quality infuses every activity in the automated information system development and maintenance efforts. The contractor shall: 1) identify opportunities for data quality improvements in all business areas for the Office of Data Architecture & Services, 2) improve regulatory compliance within USPTO by ensuring business rules are enforced at the data base level, and, 3) avoid costs associated with poor quality data. The contractor shall work in the transformation of the USPTO business into a quality-focused enterprise, supporting its strategic plan theme of "Capability."

C.3.2 RECORDS MANAGEMENT

BACKGROUND

Federal agencies are responsible for the creation, maintenance, management and disposal of federal records under their control (44 U.S.C. 3101). They are also required under the Paperwork Reduction Act of 1995 to carry out certain tasks and functions and reports.

The USPTO's federally mandated information collection program is a subset of the records management program. The information collection activities of the USPTO must meet federal requirements and it is critical that the agency is in compliance with OMB guidelines and federal laws. The PRA/Information Collection subset program's primary activity is to prepare information collection requests for the agency. Other important activities include: 1)tracking and reporting of the requests and the data associated with the agency's PRA activities. , 2) writing Privacy Act impact statements, and 3) drafting systems of records notices.

The USPTO-wide records management program supports the U.S. policy performance goal of helping to protect, promote, and expand intellectual property rights systems. The records management program represents two of the three services specified under Business Management of Information in the Federal Enterprise Architecture Business Reference Model.

3.2.1 SCOPE OF WORK – RECORDS MANAGEMENT

The contractor shall support the USPTO in records management activities agency-wide. The activities span across business areas such as (but not limited to) Patent, Trademark, Dissemination, Corporate, and Infrastructure. The contractor must have knowledge of records management tracking software and electronic document management system in general. The contractor must have experience working with Versatile software products (from Zasio). The contractor must have experience in and the ability to act as an administrator for a records management tracking system.

Records management is a USPTO-wide function that ensures compliance with federal laws and regulations and helps USPTO business areas operate more efficiently though the use of optimum records management practices. As part of this activity the contractor shall support activities of administering effective controls over the maintenance and use of federal records, as defined under the Federal Records Act and the Paperwork Reduction Act. Records are defined under 44 U.S.C 3301. The contractor shall establish and introduce procedures and techniques: 1) to improve the management of records, 2) to promote the maintenance and security of records that must be preserved, and 3) to facilitate records disposition and access. Also as part of this activity, the contractor will support the agency information collection activities under the Paperwork Reduction Act (PRA). The PRA establishes a " broad mandate for agencies to perform their information resources management activities in an efficient, effective, and economical manner." Related activities will be supported under related directives including but not limited to the Clinger Cohen Act, Paperwork Reduction Act, Privacy Act, the Government Paperwork Elimination Act, and the E-Government Act of 2002.

An active effective USPTO-wide records management program is required by law, imposed by the Office of Management and Budget (OMB), and dictated by common business sense. Such a program supports all ongoing business operations and facilitates the reengineering of the USPTO business processes. Some examples of USPTO ongoing operations and reengineering processes are: Trademark and Patent application processing, procurement, finance, human resources, patent copy sales, information technology help desk, internal correspondence, congressional correspondence, museum displays, and press releases.

The records management program is supportive of the goals of federal enterprise architecture. As specified by OMB, records ıanagement is a specific component of the framework of the Federal Enterprise business model, under Support for Delivery of Services. The Federal Enterprise Architecture Performance Management Organization defines Business Management of Information as the Information Collection, Record Retention and Information Sharing activities of a federal agency. Specifically,

" Record Retention involves managing the policies, standards, storage and security involved with the maintenance of agency data" and " Information Collection involves the day-to-day processes of gathering data from agency programs, partners and stakeholders."

The contractor shall assist the USPTO in the activities associated with a federal vital records program. A well-executed vital records program supports disaster recovery through management controls of the information that allow the agency to function in its most fundamental way. For example, the ability to track a second-copy of patent publication data would still be possible at another location if destroyed in Arlington, allowing for continuity of operations of the USPTO.

The contractor shall perform electronic records management that is crucial to successful information technology planning. This must go hand-in-hand with the development of Automated Information Systems.

The contractor shall:

- assist the USPTO in ensuring that all USPTO records are scheduled and retired or destroyed in accordance with federal law and federal guidelines;
- maintain a close and good working relationship with staff of the National Archives and Records Administration and follow USPTO and NARA procedures;
- assist USPTO staff in organizing records (such as through file plans, classification, and storage assistance) for maximum operational efficiency;
- maintain and train records coordinators located in all business areas of the USPTO;
- provide accessioning support, including the administration of the agency accessions tracking system;
- heighten awareness of proper records management procedures;
- coordinate actions between internal and external federal offices, composing and submitting information packages for OMB clearance;
- draft the agency submissions to OMB under the Information Collection Budget;
- prepare and submit documentation for agency reports and requests to OMB under the Government Paperwork Elimination Act and future reporting as required by OMB and associated with agency Information Collection activities;
- support agency activities relating to the management of federal information resources (OMB Circular A-130);
- assist the USPTO in administration of the privacy act; and
- perform all activities within specified deadlines

Future activities focus attention on the management of electronic records and the vital records program. Two potential activities are:

- the development and implementation of a USPTO-wide records filing scheme and detailed file plans; and
- the extensive review of the agency' s records series as part of a wholly updated USPTO Comprehensive Records Schedule and updated Vital Records Disaster Recovery Plan

C.4 ABILITIES OF CONTRACTOR PERSONNEL

This subsection describes the requirements specific to the type of contractor personnel needed and the overall skill requirement.)irectly applicable experience in Data Quality Management and Records Management of a similar size and scope to that at or contemplated by the USPTO is strongly preferred in terms of both overall requirements and specific staff positions.

The contractor is expected to provide trained, knowledgeable technical personnel according to the requirements of each individual task order. Therefore, the USPTO will not provide or pay for training, conferences, or seminars to be given to the contractor personnel in order for them to perform their tasks. The only exception is for USPTO-specific and specialized training not obtainable outside the USPTO (e.g., patent examination process class). If it is determined during the performance of the task order that training, conferences, or seminars are required, only the Contracting Officer may approve that training.

All contractor personnel who interface with USPTO management and technical personnel must have excellent oral and written communication skills. "Excellent oral and written communication skills" is defined as the capability to converse fluently, communicate effectively, and write intelligibly in the English language.

C.4.1 LABOR CATEGORIES

The contractor shall provide technical staff comprised of professionals in technical project leadership and a full range of Data Quality Management and Records Management disciplines. Below is a listing of the labor categories that the USPTO considers necessary under the scope of this contract. As necessary, additional labor categories may be added in order to fulfill staffing requirements under the scope of this contract.

The USPTO estimates a requirement for a total of approximately 13,500 staff hours of effort to be provided for Data Quality Management and Records Management for each year of the contract (base year plus four option years). The exact mix needed across all years of the contract cannot be precisely predicted. However, for the base year of the contract, the USPTO estimates that the following Data Quality Management and Records Management skill-sets will be required:

- Technical Program/Project Manager (500 staff hours)
- Data Quality Management Specialist
    - Senior Data Quality Management Specialist (2000 staff hours)
    - Junior Data Quality Management Specialist (2000 staff hours)
- Records Management Specialist
    - Two Senior Records Management Specialists (4000 staff hours)
    - Two Junior Records Management Specialists (4000 staff hours)
- Technical Writer/Editor (1000 staff hours)

The USPTO may shift this distribution as needed to fulfill mission objectives and to keep within budgetary constraints. Above is a listing of the labor categories that the USPTO considers necessary under the scope of this contract.

The USPTO anticipates two persons for Data Quality and four persons for Record Management, with the Program Manager and Technical writer supporting both.

C.4.1.1 KEY PERSONNEL

Key personnel shall include a Technical Program/Project Manager.

C.4.2 SPECIFIC PERSONNEL QUALIFICATIONS

The following labor categories and functional requirements have been provided for evaluation purposes. Please note that the titles of these categories are illustrative only. It is not required that the personnel of the contractors have these exact titles; rather, personnel shall meet the criteria listed below.

C.4.2.1 PROGRAM/PROJECT MANAGER (KEY PERSONNEL)

General Description

An individual who is extremely knowledgeable and skilled in managing substantial contract support services involving multiple projects and personnel. Demonstrates very good oral and written communications skills.

Function

Shall be responsible for the overall contract performance and shall not serve in any other capacity under this contract. Organizes, plans, directs, staffs, and coordinates the overall program effort; manages contract and subcontract activities as the authorized interface with the Contracting Officer, COTR, Government management personnel, and customer agency representatives; ensures compliance with Federal rules and regulations. Shall have demonstrated communications skills with all levels of management. Establishes and alters (as necessary) management structure to effectively direct contract support activities. Meets and confers with USPTO management and technical personnel regarding the status of specific contractor activities and problems, issues, or conflicts requiring resolution. Shall be capable of negotiating and making binding decisions for the company. May work as a team member.

C.4.2.2 SENIOR DATA QUALITY MANAGEMENT SPECIALIST

General Description

An individual who is very knowledgeable and skilled in all aspects of information engineering methodology and data quality analysis. Demonstrates very good oral and written communications skills.

Function

Provides competent leadership and highly specialized and technical guidance in data quality assessment of complex information systems. Plans, manages and provides technical oversight for data quality assessment activities. Certify databases are in compliance with business requirements. Provide strategic guidance for data quality program. Ensures systems are compliant with data management standards and requirements. Performs data quality analyses, using automated tools; performs information-engineering analysis of data models. Facilitates data quality assessment working sessions. Validates data conforms to structure as depicted in data models and in accordance with business rules. Provide training of data quality tools, and data quality methodology. Coordinates with the Program/Project Manager to ensure problem resolution and customer satisfaction. May work as a team member. Interfaces with Government management and technical personnel including a.) Contracting Officer (CO) and b.) Contracting Officer's Technical Representative (COTR). Reports in writing and orally to Government contract management personnel and other Government representatives.

C.4.2.3 JUNIOR DATA QUALITY MANAGEMENT SPECIALIST

General Description

An individual who is knowledgeable and also has experience in information engineering methodology and data quality assessment. Demonstrates good oral and written communications skills.

Function

Provides specialized and technical guidance to complex system data quality challenges. Ensures systems are compliant with data management standards and requirements. Performs data quality analysis, using automated tools. Performs information engineering analysis of databases. Facilitates data quality assessment working sessions. Assess, report, and certify database quality. Validates data conforms to structures as depicted in data models and in accordance with business rules. May work as a team member. Interfaces with Government management and technical personnel including the Contracting Officer and Contracting Officer's Technical Representatives. Reports in writing and orally to Government contract management personnel and other Government representatives.

C.4.2.4 SENIOR RECORDS MANAGEMENT SPECIALIST

General Description

An individual who is very knowledgeable and skilled in all aspects of Federal Records Management. Demonstrates very good oral and written communications skills.

Function

Provides highly specialized and technical guidance, to records management, disaster recovery and management of federal information resources challenges. Ensures the USPTO is compliant with federal records management and information management standards, regulations and requirements. May work as a team member. Interfaces with Government management and technical personnel including the Contracting Officer and Contracting Officer's Technical Representative. Reports in writing and orally to Government contract management personnel and other Government representatives.

C.4.2.5 JUNIOR RECORDS MANAGEMENT SPECIALIST

General Description

An individual who is knowledgeable and has experience in Federal Records Management and management of federal information resources (including the clearance process under the Paperwork Reduction Act). Demonstrates good oral and written communications skills.

Function

Provides specialized and technical solutions to the records management problems. Supports the agency business areas in records management and the management of federal information resources. May work as a team member. Interfaces with Government management and technical personnel including the Contracting Officer and Contracting Officer's Technical Representatives. Reports in writing and orally to Government contract management personnel and other Government representatives.

C.4.2.6 TECHNICAL WRITER/EDITOR

General Description

An individual who is extremely knowledgeable and skilled in technical documentation and presentation techniques, to include technical writing, technical proofreading, and technical editing. Demonstrates excellent command and articulation of the English language. Has superior grammatical skills and ability to use automated editing and publishing tools.

Function

Collects and organizes information required for preparation of deliverables; ensures the use of proper technical terminology; performs technical writing, editing, proofreading, and integration of computer-based material to produce document deliverables; and translates technical information into clear, readable documents to be used by technical and non-technical personnel. May work as a team member. Interfaces with Government management and technical personnel, and the Contracting Officer's Technical Representative (COTR). Reports in writing and orally to Government contract management personnel and other Government representatives.

C.5 EFFECTIVE PERIOD OF THIS CONTRACT

The period of performance (POP) for this contract will be five years – a base year starting at the effective date of contract award, followed by four (4) optional years. The contractor can also earn up to (4) four six month Award Terms. See Section F.4 Period of Performance

C.6 CONTRACT TYPE/ISSUANCE OF TASK ORDERS

The contract type will be a Labor Hour – Performance-Based contract with the issuance of Task Orders.

C.7 PLACE OF PERFORMANCE

The contractor shall perform the majority of the Data Quality Management and Records Management work under this Statement of Work (SOW) at the contractor's facility (unless otherwise specified in a task order). The contractor will have network access to the USPTO networks and access to specified databases as necessary to perform the tasking.

C.8 PROBLEM NOTIFICATION

A. The contractor shall notify the USPTO's Contracting Officer and COTR immediately of all problems that impact or potentially impact the contract, deliverable(s), or project schedule. Such notifications shall be made verbally during normal work hours or at the beginning of the next Government workday. For each problem encountered, verbal notification shall be followed by a written report to the Contracting Officer and copy to the COTR within 24 hours after the identification of the problem.

B. The report shall include at a minimum:

1. The nature of the problem
2. How or why the problem occurred
3. The steps being taken to correct the problem
4. The consequences of the problem
5. Actions to prevent similar occurrences.

C.9 STATUS REPORTS

A. The contractor shall submit written monthly status reports 10 calendar days after the end of each calendar month. The contractor shall prepare and submit four (4) copies to the Government, three (3) copies shall be provided to the COTR and one (1) copy to the Contracting Officer.. A status report will contain, at a minimum, the following items:

1. A summary of progress made during the month of each.
2. A summary of staff hours and funds expended during the month, expended to date, and remaining for each task and the total project.
3. A description of major difficulties that have been encountered which may delay task completion or product delivery, and statements of the steps to be taken to solve the problem.

B. If there are no problems, all monthly status reports shall include written statements, as follows, certifying to the absence of progress problem:

1. "The contractor hereby certifies that it recognizes no problems which affected progress during the current reporting period."
2. "The contractor hereby certifies that it anticipates no problems will occur during the next reporting period."

C. The status report shall be submitted in accordance with the format and criteria provided in the Monthly Status Report (Contract Deliverable No. FN01) – Section J, Attachment 1.

C.10 MEETINGS

A. When scheduled one week in advance by the COTR, the contractor shall conduct monthly Task Order Status Reviews with the USPTO's COTR or his/her representative. Subjects for discussion at the meetings shall include at a minimum; but are not limited to:

1. Work completed during the reporting period.
2. Technical status reports on all tasks.
3. Financial status reports on all tasks.
4. Work schedule for the next reporting period.
5. Identification of any problems or delays and recommendations as to their resolution with reference to the problem reports submitted in the interim.

The contractor shall make available all technical personnel associated with the project work areas, which are related to the topics that are listed in the proposed agenda.

B. Other meetings between the contractor and the USPTO will be held on an "as required" basis during the performance of the contract. The majority of the meetings will be held at the U.S. Patent and Trademark Office, 2121 Crystal Drive (Crystal Park 2), Suite 1004, Arlington, VA 22202; however, meetings may also be held at the contractor's facility when determined appropriate by the COTR. The contractor shall be able to attend any meeting called by the USPTO when given a sixty (60) minute advance notice of such a meeting.

SECTION D -- PACKAGING AND MARKING

D.1 52.252-01 CLAUSES INCORPORATED BY REFERENCE

There are no clauses incorporated in this section.

SECTION E -- INSPECTION AND ACCEPTANCE

E.1 52.252-02 CLAUSES INCORPORATED BY REFERENCE

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

http://www.arnet.gov/far/loadindex.html

Clause	Title	Date
52.246-06	Inspection--Time-And-Material And Labor-Hour	May 2001

SECTION F -- DELIVERIES OR PERFORMANCE

F.1 52.252-02 CLAUSES INCORPORATED BY REFERENCE

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

http://www.arnet.gov/far/loadindex.html

Clause	Title	Date
52.242-15	Stop-Work Order	August 1989
52.247-34	F.O.B. Destination	November 1991

F.2 DELIVERABLES

The contractor shall deliver all technical products to the USPTO as required and specified in each task order. All documentation ınd deliverables shall conform to the specifications defined within the task orders. The number of copies, specific instructions for the medium and format for electronic copies, and other instructions about deliverables will be specified in the task orders. The contractor shall provide electronic deliverables in a format compatible with the USPTO environment. As appropriate, products delivered under this contract will conform to the Technical Standards Guidelines (TSGs) Attachments 8 & 9 and follow the principles, policies, and standard stated in the Life Cycle Management (LCM) document for Automated Information Systems (AISs).

F.3 GOVERNMENT HOLIDAYS

The following legal holidays are observed by this Government agency. Holidays falling on Saturdays are observed on the Friday preceding the holiday, while those holidays falling on Sundays are observed on the Monday following the holiday.

New Year's Day	January 1
Martin Luther King, Jr.'s Birthday	Third Monday in January
President's Day	Third Monday in February
Memorial Day	Last Monday in May
Independence Day	July 4
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Veterans Day	November 11
Thanksgiving Day	Fourth Thursday in November
Christmas Day	December 25

The Contractor shall comply with the aforementioned Government holidays and any other day designated by Federal Statute, Executive Order, or Presidential proclamation, therefore, the Government offices are closed to the Contractor's staff on the day(s) these holidays are observed.

F.4 PERIOD OF PERFORMANCE

The period of performance of this contract is as follows:

CONTRACT PERIOD	PERIOD OF PERFORMANCE
Base Period	Date of award through 12 months thereafter
Option Period 1	Date of option exercise through 12 months thereafter
Option Period 2	Date of option exercise through 12 months thereafter
Option Period 3	Date of option exercise through 12 months thereafter
Option Period 4	Date of option exercise through 12 months thereafter

SECTION G -- CONTRACT ADMINISTRATION DATA

G.1 CONTRACT ADMINISTRATION

Notwithstanding the Contractor's responsibility for total management during the performance of this contract, the administration of the contract will require maximum coordination between the Government and the Contractor. The following individuals will be the Government points of contact during the performance of the contract.

(1) Contracting Officer's Technical Representative

A Contracting Officer's Technical Representative (COTR) will be designated on authority of the Contracting Officer to monitor all technical aspects and assist in administrating the contract. The types of actions within the purview of the COTR's authority are to assure that the Contractor performs the technical requirements of the contract; to maintain both written and oral communications with the Contractor concerning the aspects of the contract within his/her purview; to issue written interpretations of technical requirements of Government drawings, designs and specifications; to monitor the Contractor's performance under the contract and notify the Contractor and Contracting Officer of any deficiencies observed; and to coordinate Government-Furnished Property or Data availability and provide for site entry of Contractor personnel if required. A letter of designation will be issued to the COTR with a copy supplied to the Contractor, stating the responsibilities and limitations of the COTR. This letter will clarify to all parties to this contract the responsibilities of the COTR. At no time may the scope of work, price, delivery dates, or other mutually agreed upon terms or provisions of the contract be changed without being executed in writing by the Contracting Officer authorizing such changes.

The designated COTR is Sharon Austin, 2121 Crystal Drive, Arlington, VA. 22202 . Her phone number is 703-305-9322.

(2) Contracting Officer

All contract administration will be effected by the Contracting Officer, address as shown on the face page of this solicitation. Communications pertaining to contract administration matters will be addressed to the Contracting Officer. No changes in or deviation from the scope of work shall be effected without a Supplemental Agreement executed by the Contracting Officer authorizing such changes.

G.2 CONTRACTING OFFICER'S AUTHORITY

The Contracting Officer is the only person authorized to make or approve any changes in any of the requirements of this contract and notwithstanding any provisions contained elsewhere in this contract, the said authority remains solely in the Contracting Officer. In the event the Contractor makes any changes at the direction of any person other than the Contracting Officer, the change will be considered to have been made without authority and no adjustment will be made in the contract price to cover any increase in costs incurred as a result.

G.3 CONTRACTING OFFICER'S TECHNICAL REPRESENTATIVE (COTR)

(a) The Contracting Officer hereby designates the individual named below as the Contracting Officer's Technical Representative:

NAME: TBD
ADDRESS: U.S. Patent and Trademark Office
OCIO-Office of Acquisition Management
Crystal Park Two, Room 1002
Arlington, VA 22202

PHONE NO.: TBD

(b) The COTR may be changed at any time by the Government without prior notice to the Contractor, but notification of the change, including the name and address of the successor COTR, will be promptly provided to the Contractor by the Contracting Officer in writing.

(c) The responsibilities and limitations of the COTR are as follows:

(1) The COTR is responsible for the technical aspects of the project and technical liaison with the Contractor. The COTR is also responsible for the final inspection and acceptance of all reports, and such other responsibilities as may be specified in the contract.

(2) The COTR is not authorized to make any commitments or otherwise obligate the Government or authorize any changes which affect the Contract price, terms or conditions. Any Contractor request for changes shall be referred to the Contracting Officer directly or through the COTR. No such changes shall be made without the expressed prior authorization of the Contracting Officer. The COTR may designate assistant COTR(s) to act for her by naming such assistant in writing and transmitting a copy of such designation through the Contracting Officer to the Contractor.

G.4 INVOICING AND PAYMENT INSTRUCTIONS

The Contractor shall submit proper invoices on a monthly basis for payment. One (1) original and two (2) copies of each invoice shall be submitted with costs for each task order broken out separately (on separate pages). Invoices shall, if applicable, deduct the withholding amount as specified in FAR 52.232-7, Payments Under Time-and-Materials and Labor-Hour Contracts APR 1984, contained in Section I, "CONTRACT CLAUSES," of this contract. Depending on the mode of delivery, all invoices shall be submitted to the following address:

One copy shall be sent to the Contracting Officer at:

Courier or Hand Delivery
U.S. Patent and Trademark Office
Office of Procurement
2011 Crystal Drive - Suite 810
Arlington, VA 22202

U.S. Mail Delivery
U.S. Patent and Trademark Office
Office of Procurement
Mail Stop 6
PO Box 1450
Washington, D.C. 20231

Additionally one copy shall be sent to the Office of Finance at:

Courier or Hand Delivery
U.S. Patent and Trademark Office
Office of Finance
2011 Crystal Drive - Suite 802B
Arlington, VA 22202

U.S. Mail Delivery
U.S. Patent and Trademark Office
Office of Finance
Mail Stop 17
PO Box 1450
Washington, D.C. 20231

To constitute a proper invoice, each invoice submitted must include the following information and attached documentation:

(1) Name of the Contractor, invoice number and invoice data;
(2) Contract number and task order numbers;
(3) Description, price, and quantity of services actually delivered or rendered;
(4) Name of personnel performing the service, Labor-Hour Category, number of hours worked and cost;
(5) Payment terms;

(6) Name and signature of certifying official, title, phone number, and complete mailing address of responsible office to whom payment is to be sent;

(7) Period of performance covered by the invoice;

(8) Other substantiating documentation or information as required by the contract; and

(9) The following statement on the reverse of the original of each invoice:

COTR'S CERTIFICATION

I certify to the best of my knowledge and belief that the services shown on the invoice have been performed and are accepted.

____________________ __________
COTR Signature Date

G.5 RESERVED

G.6 ELECTRONIC PAYMENT INFORMATION

(a) The information required by the clause at FAR 52.232-34, Payment by Electronic Funds Transfer-Other Than Central Contractor Registration (see Section I), shall be forwarded by the Contractor to the below-designated office:

U.S. Patent and Trademark Office
Office of Finance, Box 17
Crystal Park One, Room 802B
Washington, D.C. 20231

(b) If requested, a form will be provided to the Contractor for this purpose. In the event payment is assigned to a bank, thrift, or other financing institution pursuant to the clause FAR 52.232-23, Assignment of Claims (see Section I), the Contractor shall forward that form to the assignee for completion.

G.7 SEGREGATION OF COSTS BY TASK ORDER

As referenced in clause G.4, all costs shall be accumulated by individual task order number and billed on one monthly invoice.

G.8 GOVERNMENT FURNISHED SPACE/MATERIALS

The work under this contract is to be performed primarily at the contractor's facility (unless otherwise specified in the task order). The majority of meetings will be held at the USPTO offices (currently located in Crystal City, Arlington, VA, but sometime in 2004 will be located in Alexandria, VA); however, meetings may also be held at the contractor's facility when determined appropriate by the COTR. Due to the nature of work to be performed under this contract, the contractor shall be able to attend any meeting called by the USPTO when given a 60-minute advance notice of such a meeting.

As specified in individual task orders, contractor staff occasionally may be required to temporarily work at a site specified and provided by the Government. The Government will furnish the necessary office space, office furniture, equipment, and telephones as required, on-site to meet contract requirements. Any facilities and/or equipment provided to the contractor by the Government shall be used exclusively for the performance of contract tasks.

Individual task orders will list any Government equipment or property to be provided to the contractor for use in the performance of this contract. This property shall be used and maintained by the contractor in accordance with provisions of the "Government Property" clause. Such equipment shall be returned by the contractor to the Government upon conclusion of the task order or as otherwise specified. Contractors shall provide for time and use of appropriate personnel during the USPTO's physical inventory at the contractor site of all Government furnished equipment, hardware and software at the end of each fiscal year and shall provide written reports (in a format to be provided by the COTR) upon request, of current inventory of GFE in the contractor's possession.

SECTION H – SPECIAL CONTRACT REQUIREMENTS

H.1 TYPE OF CONTRACT

This is a Labor-Hour type contract with Performance Incentives.

(a) The following are the Performance Incentives:

(i) From date of contract award, there will be a semi-annual Performance Evaluation to decide what the Performance Level rating the contractor has earned for each six (6) month period.

The Performance Levels Ratings are:

1. Excellent
2. Good
3. Unsatisfactory

(ii) The contractor will not be able to earn any Award Term extensions during the first year of this contract nor will the contractor be penalized during the first year of this contract, regardless of the Performance Level Rating they receive from the USPTO.

(iii) Beginning with the second year of the contract, the contractor may begin to earn Award Term contract extensions (in 6 months increments). Award Term contract extensions will only be awarded if the contractor receives two (2) consecutive "Excellent" Performance Level Ratings in a row.

A maximum of (4) four 6-month periods can be earned. The contractor can earn an award during the actual award term periods, if they have not yet earned all four terms.

(iv) After a six (6) month Award Term extension is given for two (2) Excellent Performance Level ratings in a row, the evaluation term starts anew.

(v) The maximum amount of Award Term contract extension time that can be earned is two (2) years.

(vi) If during the six (6) month Award Fee period, the contractor receives an Unsatisfactory Performance Level rating, the contractor will be penalized 6% of the cumulative labor hour prices charged during the award fee period.

(vii) If the contractor is rated and receives an Unsatisfactory Performance Level rating two (2) consecutive Award Fee Periods, the contractor will lose an Award Fee Terms (in six month increments) only if they have already earned a six month extension. After a six (6) month Award Term has been forfeited for the two (2) consecutive Unsatisfactory Performance Level ratings in a row, the evaluation term starts anew.

(viii) If during an Award Fee period, the PTO deems any task to be rated unsatisfactory, the overall Performance Level rating for the Award Fee period cannot be Excellent.

(ix) All earned "periods of performance" are subject to availability of subsequent fiscal year funding and continuation of a valid contract requirement

H.2 ORGANIZATIONAL CONFLICT OF INTEREST

(a) The Contractor warrants that, to the best of the Contractor's knowledge and belief, there are no relevant facts or circumstances which could give rise to an organizational conflict of interest, as defined in FAR Subpart 9.5, or that the Contractor has disclosed all such relevant information.

(b) Prior to commencement of any work, the Contractor agrees to notify the Contracting Officer immediately that, to the best of its knowledge and belief, no actual or potential conflict of interest exists or to identify to the Contracting Officer any actual or potential conflict of interest the firm may have. In emergency situations, however, work may begin but notification shall be made within five (5) working days.

(c) The Contractor agrees that if an actual or potential organizational conflict of interest is identified during performance, the Contractor will immediately make a full disclosure in writing to the Contracting Officer. This disclosure shall include a description of actions which the Contractor has taken or proposes to take, after consultation with the Contracting Officer, to avoid, mitigate, or
neutralize the actual or potential conflict of interest. The Contractor shall continue performance until notified by the Contracting Officer of any contrary action to be taken.

(d) Remedies - The USPTO may terminate this contract for convenience, in whole or in part, if it deems such termination necessary to avoid an organizational conflict of interest. If the Contractor was aware of a potential organizational conflict of interest prior to award or discovered an actual or potential conflict after award and did not disclose it or misrepresented relevant information to the Contracting Officer, the Government may terminate the contract for default.

(e) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder provisions which shall conform substantially to the language of this clause, including this paragraph, unless otherwise authorized by the Contracting Officer.

H.3 LIMITATION OF FUTURE CONTRACTING

(a) The parties to this contract agree that the Contractor will be restricted in its future contracting in the manner described below. Except as specifically provided in this clause, the Contractor shall be free to compete for contracts on an equal basis with other companies.

(b) If the Contractor, under the terms of this contract, or through the performance of work pursuant to this contract, is required to prepare or assist in preparing specifications or statements of work and such specifications or statements of work are incorporated into an USPTO solicitation, the Contractor shall be ineligible to perform the work described in that solicitation as a prime Contractor or subcontractor under an ensuing USPTO contract.

H.4 KEY PERSONNEL

A. The Contractor shall assign to this contract the following key personnel:

(1) Technical Project Manager

B. During the first 180 days of performance, the Contractor shall make no substitutions of key personnel unless the substitution is necessitated by illness, death or termination of employment. The Contractor shall notify the CO within fifteen (15) calendar days after the occurrence of any of these events and provide the information required by paragraph (c) below. After the initial 180-day period, the Contractor shall submit the information required by paragraph (c) to the CO at least 15 days prior to making any permanent substitutions.

C. The Contractor shall provide a detailed explanation of the circumstances necessitating the proposed substitutions, complete resumes for the proposed substitutes, and any additional information requested by the CO. Proposed substitutes should have comparable qualifications to those of the persons being replaced. The CO will notify the Contractor within fifteen (15) calendar days after receipt of all required information of the decision on substitutions. The contract will be modified to reflect any approved changes of key personnel.

H.5 DUPLICATION AND DISCLOSURE OF CONFIDENTIAL DATA

Duplication or disclosure of confidential data provided by the PTO or to which the Contractor will have access as a result of this contract is prohibited. It is understood that throughout performance of the contract, the Contractor may have access to confidential data that is the sole property of the PTO, as well as access to proprietary data, which is the sole property of other than the contracting parties. The Contractor hereby agrees to maintain the confidentiality of all such data to which access may be gained throughout contract performance whether title thereto vests in the PTO or otherwise. The Contractor hereby agrees not to disclose said data, any interpretations thereof, or data derivative there from, to unauthorized parties in contravention of these provisions without prior written approval of the Contracting Officer or the party in which title thereto is wholly vested. This clause also applies to any subcontractors and consultants used by the Contractor.

The contractor shall obtain from each employee who has access to proprietary data under this contract, a written agreement in which shall in substance provide that such employee shall not, during his/her employment by the contractor or thereafter, disclose to others or use for their benefit, proprietary data received in connection with the work under this contract. Furthermore, the contractor will instill in its employees the philosophy of Part 9.505-4 of the Federal Acquisition Regulation so that they will not use or disclose proprietary information or data generated or acquired in performance of this contract except as provided herein.

Upon completion or termination of this contract, the Contractor shall return to the Government all GFD.

H.6 GOVERNMENT FURNISHED DATA

The Government shall deliver to the Contractor, as may be requested, Government-Furnished Data (GFD) during the performance of this contract. GFD will be delivered to the Contractor as specified in each task order.

Title to GFD shall remain in the Government, and the Contractor shall use the GFD only in connection with this contract.

Upon Complettion or termination of this contract, the Contractor shall return the Gvoernment all GFD..

H.7 OVERTIME

Unless otherwise provided in this contract, the Contractor shall not perform overtime work under or in connection with this contract for which premium compensation is required to be paid, without specific written approval from the Contracting Officer.

H.8 ADVERTISING OF AWARD

The Contractor agrees not to refer to awards in commercial advertising in such manner as to state or imply that the services provided are endorsed or preferred by the Federal Government, it is considered by the Government to be superior to other services. Advertisements, press releases, and publicity of a contract by a supplier shall not be made without the prior express written permission of the Contracting Officer.

H.9 SECRECY AND USAGE OF PATENT INFORMATION

(a) Patent applications are required by law (35 U.S.C. 122) to be kept in confidence. In addition pursuant to secrecy order provisions of 35 U.S.C. 181-188, work under this contract may affect national security. Information contained in any patent application file(s) are restricted to authorized Contractor personnel having a need to know.

(b) The Contractor acquires no right or privilege to use or disclose any information contained in any patent file (in any form whatsoever) except to perform the work under this contract. Further, the Contractor shall not copyright or make any use or disclose whatsoever of any patent information contained in any application or related copy or data furnished the Contractor by the Government or obtained therefrom except for performing the work procured under this contract.

(c) Patent documents or copies of information contained therein, patent applications and abandoned files, when furnished to the Contractor by the PTO, shall be handled in accordance with the provisions of:

(1) 35 U.S.C. §122
(2) 37 CFR §1.14
(3) 35 U.S.C. §181-188

(d) All personnel employed in data preparation work on this contract, or otherwise having access to patent files or data or information concerning the same shall take the following oath, or affirmation, signed in writing:

"I do swear or affirm that I will preserve application for patents in secrecy, that I will not divulge any information concerning the same to unauthorized persons while employed in work under Contract 50-PAPT-#-#### or any time thereafter, and that I take this obligation freely, and without any mental reservation or purpose of evasion."

(e) Each employee's signed oath, or affirmation, shall be retained in the Contractor's files, subject to inspection by authorized Government representatives.

(f) Without advance notice, the Government shall have the right to inspect the Contractor's premises, records, and work in process pertaining to the secrecy of patent information.

(g) The Contractor shall submit, for approval by the COTR, a plan for maintaining the confidentiality of patent documents and all information contained therein. The plan must adequately protect documents, film and all other communications and storage media during all phases of staging, filming, handling, processing, storage and quality control. This plan shall be submitted to the COTR thirty (30) calendar days after contract award

(h) Duplication of confidential material by the Contractor is forbidden except as specified in this contract.

(I) The Contractor shall transport all documents, film and all other communications and storage media used in the performance of this contract between the Contractor's work site and the PTO. This includes pickup of work to be done from PTO offices and delivery of completed work to designated PTO offices.

(j) The Contractor shall be responsible for returning all Government Furnished Patent Document items to the Government upon termination of the contract in accordance with the Government-Furnished Data clause of this contract.

(k) The Contractor shall insert the substance of this clause in each subcontract hereunder unless the Contracting Officer has waived this requirement, in writing, as to particular subcontracts or classes of subcontracts.

H.10 ACCESS TO GOVERNMENT FACILITIES

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

H.11 GOVERNMENT IDENTIFICATION/SUITABILITY INVESTIGATION REQUIREMENTS

Each contract employee working under this contract must undergo investigative processing. The investigation that will be conducted by the Office of Personnel Management (OPM) is a National Agency Check with Inquires (NACI).

Investigative Processing -
The Contractor's Project Manager is responsible for initiating and ensuring the accuracy and completeness of the investigative package for each contract employee. Once the packages have been reviewed, packages will then be forwarded to the USPTO Security Office for further processing, e.g., fingerprinting, etc. Investigative paperwork must be submitted to the USPTO Security Office and forwarded to the OPM within 14 days after the Subject's performance on the contract.
Processing Requirements -
The investigative package must contain the following investigative forms: SF-85, Questionnaire for Non Sensitive Positions; FD 258, Fingerprint Chart; and the OF 306, Declaration for Federal Employment.
Non U.S. citizens to be employed under this contract must:
a. Have official legal status in the United States; and
b. Have continuously resided in the United States for the last 2 years

If the USPTO Security Office receives disqualifying information on a contract employee, the Contractor, upon notice, will immediately remove the employee from their duties under this contract. Contract employees may be barred from working on the premises of a facility for any of the following:

a. Falsification of information entered on the investigative forms.

b. Conviction of a felony of a crime of violence or of a misdemeanor involving moral turpitude.

c. Improper conduct once performing on the contract, including criminal, infamous, immoral, or notoriously disgraceful conduct or other conduct prejudicial to the Government regardless of whether the conduct directly relates to the contract.

d. Any behavior judged to pose a potential threat to USPTO personnel or property.
Failure to comply with these requirements may result in the cancellation of this contract.

H. 12 SECRECY AND USAGE OF PATENT INFORMATION

Work under this contract does not affect the national security. However, patent applications are required by law (35 U.S.C. 122) to be kept in confidence. Information contained in any patent application file(s) is restricted to authorized Contractor personnel on a need-to-access basis.

The Contractor acquires no right or privilege to use or disclose any information contained in any patent application file (in any form whatsoever) except to perform the work under the contract. Further, the Contractor shall not copyright or make any use or disclosure whatsoever of any patent information contained in any application or related copy or data furnished the Contractor by the Government or obtained therefrom except performing the requirements of this contract.

Security requirements of patent application file data maintained in a computer-accessible medium are an extension of the security requirements for the hard copy or the patent application folders. All processing, storage or transmission of patent application file data by means of electronic communications systems is prohibited unless use of such systems is approved by the USPTO.

All personnel having access to patent application files or data or information concerning the same, must take the following at or affirmation, signed in writing:

"I do swear or affirm that I will preserve the applications for patents in secrecy, that I will not divulge any information concerning the same to unauthorized persons while employed in work under this contract or at any time thereafter; and that I take this obligation freely, and without mental reservation or purpose of evasion."

Each employee's signed oath, or affirmation, shall be retained in the Contractor's file, subject to inspection by authorized Government representatives.

Without advance notice, the Government shall have the right to inspect the Contractor's premises, records, and work in process pertaining to the secrecy of patent information.

H.13 CAR 1352.239-73- SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY RESOURCES

(a) This clause is applicable to all contracts that include information technology resources or services in which the Contractor must have physical or electronic access to USPTO's sensitive or classified information, which is contained in systems that directly support the mission of the Agency. For purposes of this clause the term "Sensitive" is defined by the guidance set forth in:
(1) The DOC IT Security Program Policy and Minimum Implementation Standards (http://www.osec.doc.gov/cio/itmhweb/itmhweb1.html);
(2) The Office of Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Resources, (http://csrc.nist.gov/secplcy/a130app3.txt) which states that there is a "presumption that all [general support systems] contain some sensitive information."; and
(3) The Computer Security Act of 1987 (P.L. 100-235) (http://www.epic.org/crypto/csa/csa.html), including the following definition of the term sensitive information "... any information, the loss, misuse, or unauthorized access, to or modification of which could adversely affect the national interest or the, conduct of federal programs, or the privacy to which individuals are entitled under section 552 a of title 5, Unites States Code (The Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."

For purposes of this clause, the term "Classified" is defined by the guidance set forth in:
(1) The DOC IT Security Program Policy and Minimum Implementation Standards, Section 3.3.1.4 (http://www.osec.doc.gov/cio/itmhweb/itmhweb1.html).
(2) The DOC Security Manual, Chapter 18 (http://www.osec.doc.gov/osy/).
(3) Executive Order 12958, as amended, Classified National Security Information. Classified or national security information is information that has been specifically authorized to be protected from unauthorized disclosure in the interest of national defense or foreign policy under an Executive Order or Act of Congress.

Information technology resources include, but are not limited to, hardware, application software, system software, and information (data). Information technology services include, but are not limited to, the management, operation (including input, processing, transmission, and output), maintenance, programming, and system administration of computer systems, networks, and telecommunications systems. The Contractor shall be responsible for implementing sufficient Information Technology security, to reasonably prevent the compromise of USPTO IT resources for all of the contractor's systems that are interconnected with a USPTO network or USPTO systems that are operated by the Contractor.

b) All Contractor personnel performing under this contract and Contractor equipment used to process or store USPTO data, or to connect to USPTO networks, must comply with the requirements contained in the USPTO IT Security Handbook.

(c) For all Contractor-owned systems for which performance of the contract requires interconnection with a USPTO network or that USPTO data be stored or processed on them, the Contractor Shall:

(1) Provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract. The plan shall describe those parts of the contract to which this clause applies. The Contractor's IT Security Plan shall comply with federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.) and the Federal Information Security Management Act of 2002, Pub. L. No.107-347, 116 Stat. 2899, 2946-2961 (2002); Pub. L. No. 107-296, 116 Stat. 2135, 2259-2273 (2002). 38 WEEKLY COMP. PRES. DOC. 51, 2174 (Dec. 23, 2002) (providing statement by President George W. Bush regarding Federal Information Security Management Act of 2002). The plan shall meet IT security requirements in accordance with Federal and USPTO policies.and procedures that include, but are not limited to:

(a) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources
(http://csrc.nist.gov/secplcy/a130app3.txt);
(b) National Institute of Standards and Technology Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems (http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF) ; and
(c) DOC Procedures and Guidelines in the Information Technology Management Handbook
(http://www.osec.doc.gov/cio/itmhweb/itmhweb1.html)..
(d) National Industrial Security Program Operating Manual (NISPOM) for classified systems
(http://www.dss.mil/isec/nispom.htm); and

(2) Within 14 days after contract award, the contractor shall submit for USPTO approval a System Certification and Accreditation package, including the IT Security Plan and a system certification test plan, as outlined in USPTO Certification and Accreditation Technical Standard and Guideline. The Certification and Accreditation Package must be consistent with and provide further detail for the security approach contained in the offeror's proposal or sealed bid that resulted in the award of this contract and in compliance with the requirements stated in this clause. The Certification and Accreditation Package, as approved by the Contracting Officer, in consultation with the USPTO IT Security Officer, shall be incorporated as part of the contract. USPTO will use the incorporated IT Security Plan as the basis for certification and accreditation of the contractor system that will process USPTO data or connect to USPTO networks. Failure to submit and receive approval of the Certification and Accreditation Package, as outlined above may result in termination of the contract.

(d) The Contractor shall incorporate this clause in all subcontracts that meet the conditions in paragraph (a) of this clause.

H. 14 CAR 1352.239-74 SECURITY PROCESSING REQUIREMENTS FOR CONTRACTORS/SUBCONTRACTOR PERSONNEL FOR ACCESSING USPTO AUTOMATED INFORMATION SYSTEMS

(a) Contractor personnel requiring any access to AISs operated by the Contractor for USPTO or interconnected to a USPTO network to perform contract services shall be screened at an appropriate level in accordance with Commerce Acquisition Manual 1337.70, *Securit Processing Requirements for Service Contracts*. USPTO shall provide screening using standard personnel screening forms, which the Contractor shall submit to the USPTO Contracting Officer's Technical Representative (COTR) based on the following guidance:

1) **Contract personnel performing work designated Contract High Risk and personnel performing work designated Contract Moderate Risk in the information technology (IT) occupations and those with "global access" to an automated information AIS require a favorable pre-employment check before the start of work on the contract, regardless of the expected duration of the contract. After a favorable pre-employment check has been obtained, the Background Investigation (BI) for Contract High Risk and the Minimum Background Investigation (MBI) for Contract IT Moderate Risk positions must be initiated within three working days of the start of work.**

2) **Contract personnel performing work designated Contract Moderate Risk who are not performing IT-related contract work do not require a favorable pre-employment check prior to their employment; however, the Minimum**

Background Investigation (MBI) must be initiated within three working days of the subject's start of work on the contract, regardless of the expected duration of the contract.

3) **Contract personnel performing work designated Contract Low Risk will require a National Agency Check and Inquiries (NACI) upon the subject's start of work on the contract if the expected duration of the contract exceeds 365 calendar days. The NACI must be initiated within three working days of the subject's start of work on the contract.**

4) **Contract personnel performing work designated Contract Low Risk will require a Special Agreement Check (SAC) upon the subject's start of work on the contract if the expected duration of the contract (including options) exceeds 180 calendar days but is less than 365 calendar days. The SAC must be initiated within three working days of the subject's start of work on the contract.**

5) **Contract personnel performing work on contracts requiring access to classified information must undergo investigative processing according to the Department of Defense National Industrial Security Program Operating Manual (NISPOM), (http://www.dss.mil/isec/nispom.htm) and be granted eligibility for access to classified information prior to beginning work on the contract.**

The security forms may be obtained from USPTO Office of Security. At the option of the government, interim access to USPTO AISs may be granted pending favorable completion of a pre-employment check. Final access may be granted only on completion of an appropriate investigation based upon the risk level assigned to the contract.

Within 5 days of contract award, the Contractor shall certify in writing to the COTR that its employees, in performance of the contract, have completed annual IT security awareness training in USPTO IT Security policies, procedures, computer ethics, and best practices, in accordance with the USPTO Training Policy. The COTR will inform the Contractor of any other available USPTO training resources.

(c) Within 5 days of contract award, the Contractor shall provide the COTR with signed Nondisclosure .greements as specified in Commerce Acquisition Regulation (CAR), 1352.209-72, *Restrictions Against Disclosures*.

(d) The Contractor shall afford USPTO, including the Office of Inspector General, access to the Contractor's and subcontractor's facilities, installations, operations, documentation, databases, and personnel used in performance of the contract. Access shall be provided to the extent required to carry out a program of IT inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of USPTO data or to the function of computer AISs operated on behalf of USPTO, and to preserve evidence of computer crime.

The Contractor shall incorporate this clause in all subcontracts that meet the conditions in paragraph (a) of this clause.

)TE: Low Risk contracts whose duration is less than 180 days do not ordinarily require security processing. However, even though the contract is short in duration, based on any unusual circumstances that may exist, Special Agreement Checks (SACs) may be requested, at the discretion of the Contracting Officer's Technical Representative (COTR) and/or the USPTO Security Office.)

H.15 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT MARCH 2000

(a) The Government may unilaterally extend the term of this contract by written notice to the Contractor prior to the end of the current period of performance, provided that the Government gives the Contractor a preliminary written notice of its intent to tend at least 30 days before the contract expires. The preliminary notice does not commit the Government to an extension.
(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.
(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed five (5) years plus up to four six month award terms if earned.

H.16 SECTION 508 OF THE REHABILITATION ACT OF 1973 COMPLIANCE

In accordance with Section 508, Subsection 508 (a)(3), the USPTO requires that all Electronic Information Technology ("EIT"), as that term is defined at FAR 2.101, delivered under this contract comply with the applicable EIT technology accessibility standards issued by the Architectural and Transportation Barriers Compliance Board set forth at 36 CFR Part 1194.

H.17 IT SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES

A. This clause is applicable to all or any part of the contract that includes information technology resources or service in which the contractor must have physical or electronic access to USPTO's sensitive information contained in unclassified systems that directly support the mission of the Agency. This includes information technology, hardware, software, and the management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunication systems.

B. Within 30 days of contract award, the contractor shall certify in writing to the COTR that its employees, in performance of the contract, have completed:

1. USPTO IT Security User Awareness Training
2. Annual IT Security training USPTO IT Security policies, computer ethics, and best practices (when available).

The contractor may use web-based training as available from USPOT to meet these requirements. For contracts extending beyond one year, the contractor shall certify in writing to the COTR within the first 30 days of each contract or option year subsequent to the award year, that its employees, in performance of the contract, have completed annual IT Security User Awareness training in accordance with USPTO requirements.

C. All Contractor employees are expected to comply with USPTO's IT Security Policies.

D. The Contractor shall incorporate the substance of this clause in all subcontracts that meet the conditions in paragraph (a) of this clause.

H.18 FAR 52.224-1 PRIVACY ACT NOTIFICATION (APR 1984)

The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.
(End of clause)

H.19 FAR 224-2 PRIVACY ACT. (APR 1984)

(a) The Contractor agrees to-

(1) Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies-

(i) The systems of records; and
(ii) The design, development, or operation work that the contractor is to perform;

(2) Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a system of records on individuals that is subject to the Act; and
(3) Include this clause, including this paragraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a system of records.

(b) In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a system of records on individuals to accomplish an agency function, the Contractor is considered to be an employee of the agency.
(c)(1) "Operation of a system of records," as used in this clause, means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.

(2) "Record," as used in this clause, means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains the person's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voiceprint or a photograph.
(3) "System of records on individuals," as used in this clause, means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

SECTION I -- CONTRACT CLAUSES

I.1 52.252-02 CLAUSES INCORPORATED BY REFERENCE

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

http://www.arnet.gov/far/loadindex.html

Clause	Title	Date
52.202-01	Definitions	December 2001
52.203-03	Gratuities	April 1984
52.203-05	Covenant Against Contingent Fees	April 1984
52.203-07	Anti-Kickback Procedures	July 1995
52.204-04	Printed or Copied Double-Sided on Recycled Paper.	August 2000
52.209-06	Protecting the Government's Interest When Subcontracting With Contractors Debarred, Suspended, or Proposed for Debarment	July 1995
52.215-08	Order of Precedence--Uniform Contract Format	October 1997
52.217-09	Option To Extend The Term Of The Contract	March 2000
52.219-08	Utilization of Small Business Concerns	October 2000
52.219-14	Limitations on Subcontracting	December 1996
52.222-21	Prohibition of Segregated Facilities	February 1999
52.222-26	Equal Opportunity	April 2002
52.222-35	Equal Opportunity for Special Disabled Veterans, Veterans of the Vietnam Era, and Other Eligible Veterans	December 2001
52.222-36	Affirmative Action For Workers with Disabilities	June 1998
52.222-37	Employment Reports on Special Disabled Veterans, Veterans of the Vietnam Era, and Other Eligible Veterans	December 2001
52.223-06	Drug Free Workplace	May 2001
52.225-13	Restrictions on Certain Foreign Purchases	July 2000
52.227-14	Rights in Data—General	June 1987
52.232-07	Payments Under Time-And-Materials And Labor Hour Contracts	February 2002
52.232-17	Interest	June 1996
52.232-23	Assignment Of Claims	January 1986
52.232-25	Prompt Payment	February 2002
52.232-33	Payment by Electronic Funds Transfer-Central Contractor Registration.	October 2003
52.233-01	Disputes	December 1998
52.233-03	Protest After Award	August 1996
52.242-13	Bankruptcy	July 1995
52.243-03	Changes--Time-And-Material Or Labor-Hours	September 2000
52.249-14	Excusable Delays	April 1984
52.253-01	Computer Generated Forms	January 1991

I.2 52.203-08 CANCELLATION, RESCISSION, AND RECOVERY OF FUNDS FOR ILLEGAL OR IMPROPER ACTIVITY JANUARY 1997

(a) If the Government receives information that a contractor or a person has engaged in conduct constituting a violation of subsection (a), (b), (c), or (d) of Section 27 of the Office of Federal Procurement Policy Act (41 U.S.C. 423) (the Act), as amended by section 4304 of the 1996 National Defense Authorization Act for Fiscal Year 1996 (Pub. L. 104-106), the Government may--

(1) Cancel the solicitation, if the contract has not yet been awarded or issued; or

(2) Rescind the contract with respect to which--

(i) The Contractor or someone acting for the Contractor has been convicted for an offense where the conduct constitutes a violation of subsection 27 (a) or (b) of the Act for the purpose of either--

(A) Exchanging the information covered by such subsections for anything of value; or

(B) Obtaining or giving anyone a competitive advantage in the award of a Federal agency procurement contract; or

(ii) The head of the contracting activity has determined, based upon a preponderance of the evidence, that the Contractor or someone acting for the Contractor has engaged in conduct constituting an offense punishable under subsections 27(e)(1) of the Act.

(b) If the Government rescinds the contract under paragraph (a) of this clause, the Government is entitled to recover, in addition to any penalty prescribed by law, the amount expended under the contract.

(c) The rights and remedies of the Government specified herein are not exclusive, and are in addition to any other rights and remedies provided by law, regulation, or under this contract.

I.3 52.203-10 PRICE OR FEE ADJUSTMENT FOR ILLEGAL OR IMPROPER ACTIVITY JANUARY 1997

(a) The Government, at its election, may reduce the price of a fixed-price type contract and the total cost and fee under a cost-type contract by the amount of profit or fee determined as set forth in paragraph (b) of this clause if the head of the contracting activity or designee determines that there was a violation of subsection 27 (a), (b), or (c) of the Office of Federal Procurement Policy Act, as amended (41 U.S.C. 423), as implemented in section 3.104 of the Federal Acquisition Regulation.

(b) The price or fee reduction referred to in paragraph (a) of this clause shall be--

(1) For cost-plus-fixed-fee contracts, the amount of the fee specified in the contract at the time of award;

(2) For cost-plus-incentive-fee contracts, the target fee specified in the contract at the time of award, notwithstanding any minimum fee or "fee floor" specified in the contract;

(3) For cost-plus-award-fee contracts--

(i) The base fee established in the contract at the time of contract award;

(ii) If no base fee is specified in the contract, 30 percent of the amount of each award fee otherwise payable to the Contractor for each award fee evaluation period or at each award fee determination point.

(4) For fixed-price-incentive contracts, the Government may--

(i) Reduce the contract target price and contract target profit both by an amount equal to the initial target profit specified in the contract at the time of contract award; or

(ii) If an immediate adjustment to the contract target price and contract target profit would have a significant adverse impact on the incentive price revision relationship under the contract, or adversely affect the contract financing provisions, the Contracting Officer may defer such adjustment until establishment of the total final price of the contract. The total final price established in accordance with the incentive price revision provisions of the contract shall be reduced by an amount equal to the initial target profit specified in the contract at the time of contract award and such reduced price shall be the total final contract price.

(5) For firm-fixed-price contracts, by 10 percent of the initial contract price or a profit amount determined by the Contracting Officer from records or documents in existence prior to the date of the contract award.

(c) The Government may, at its election, reduce a prime contractor's price or fee in accordance with the procedures of paragraph (b) of this clause for violations of the Act by its subcontractors by an amount not to exceed the amount of profit or fee reflected in the subcontract at the time the subcontract was first definitively priced.

(d) In addition to the remedies in paragraphs (a) and (c) of this clause, the Government may terminate this contract for default. The rights and remedies of the Government specified herein are not exclusive, and are in addition to any other rights and remedies provided by law or under this contract.

I.4 52.203-12 LIMITATION ON PAYMENTS TO INFLUENCE CERTAIN FEDERAL TRANSACTIONS JUNE 1997

(a) Definitions.

"Agency," as used in this clause, means executive agency as defined in 2.101.

"Covered Federal action," as used in this clause, means any of the following Federal actions:

(1) The awarding of any Federal contract.

(2) The making of any Federal grant.

(3) The making of any Federal loan.

(4) The entering into of any cooperative agreement.

(5) The extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.

"Indian tribe" and "tribal organization," as used in this clause, have the meaning provided in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450B) and include Alaskan Natives.

"Influencing or attempting to influence," as used in this clause, means making, with the intent to influence, any communication to or appearance before an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with any covered Federal action.

"Local government," as used in this clause, means a unit of government in a State and, if chartered, established, or otherwise recognized by a State for the performance of a governmental duty, including a local public authority, a special district, an intrastate district, a council of governments, a sponsor group representative organization, and any other instrumentality of a local government.

"Officer or employee of an agency," as used in this clause, includes the following individuals who are employed by an agency:

(1) An individual who is appointed to a position in the Government under title 5, United States Code, including a position under a temporary appointment.

(2) A member of the uniformed services, as defined in subsection 101(3), title 37, United States Code.

(3) A special Government employee, as defined in section 202, title 18, United States Code.

(4) An individual who is a member of a Federal advisory committee, as defined by the Federal Advisory Committee Act, title 5, United States Code, appendix 2.

"Person," as used in this clause, means an individual, corporation, company, association, authority, firm, partnership, society, State, and local government, regardless of whether such entity is operated for profit, or not for profit. This term excludes an Indian tribe, tribal organization, or any other Indian organization with respect to expenditures specifically permitted by other Federal law.

"Reasonable compensation," as used in this clause, means, with respect to a regularly employed officer or employee of any person, compensation that is consistent with the normal compensation for such officer or employee for work that is not furnished to, not funded by, or not furnished in cooperation with the Federal Government.

"Reasonable payment," as used in this clause, means, with respect to professional and other technical services, a payment in an amount that is consistent with the amount normally paid for such services in the private sector.

"Recipient," as used in this clause, includes the Contractor and all subcontractors. This term excludes an Indian tribe, tribal organization, or any other Indian organization with respect to expenditures specifically permitted by other Federal law.

"Regularly employed," as used in this clause, means, with respect to an officer or employee of a person requesting or receiving a Federal contract, an officer or employee who is employed by such person for at least 130 working days within 1 year immediately preceding the date of the submission that initiates agency consideration of such person for receipt of such contract. An officer or employee who is employed by such person for less than 130 working days within 1 year immediately preceding the date of the submission that initiates agency consideration of such person shall be considered to be regularly employed as soon as he or she is employed by such person for 130 working days.

"State," as used in this clause, means a State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, a territory or possession of the United States, an agency or instrumentality of a State, and multi-State, regional, or interstate entity having governmental duties and powers.

(b) Prohibitions.

(1) Section 1352 of title 31, United States Code, among other things, prohibits a recipient of a Federal contract, grant, loan, or cooperative agreement from using appropriated funds to pay any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with any of the following covered Federal actions: the awarding of any Federal contract; the making of any Federal grant; the making of any Federal loan; the entering into of any cooperative agreement; or the modification of any Federal contract, grant, loan, or cooperative agreement.

(2) The Act also requires Contractors to furnish a disclosure if any funds other than Federal appropriated funds (including profit or fee received under a covered Federal transaction) have been paid, or will be paid, to any person for influencing or attempting to nfluence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with a Federal contract, grant, loan, or cooperative agreement.

(3) The prohibitions of the Act do not apply under the following conditions:

(i) Agency and legislative liaison by own employees.

(A) The prohibition on the use of appropriated funds, in subparagraph (b)(1) of this clause, does not apply in the case of a payment of reasonable compensation made to an officer or employee of a person requesting or receiving a covered Federal action if the payment is for agency and legislative liaison activities not directly related to a covered Federal action.

(B) For purposes of subdivision (b)(3)(i)(A) of this clause, providing any information specifically requested by an agency or Congress is permitted at any time.

(C) The following agency and legislative liaison activities are permitted at any time where they are not related to a specific solicitation for any covered Federal action:

(1) Discussing with an agency the qualities and characteristics (including individual demonstrations) of the person's products or services, conditions or terms of sale, and service capabilities.

(2) Technical discussions and other activities regarding the application or adaptation of the person's products or services for an agency's use.

(D) The following agency and legislative liaison activities are permitted where they are prior to formal solicitation of any covered Federal action--

(1) Providing any information not specifically requested but necessary for an agency to make an informed decision about initiation of a covered Federal action;

(2) Technical discussions regarding the preparation of an unsolicited proposal prior to its official submission; and

(3) Capability presentations by persons seeking awards from an agency pursuant to the provisions of the Small Business Act, as amended by Pub. L. 95-507, and subsequent amendments.

(E) Only those services expressly authorized by subdivision (b)(3)(i)(A) of this clause are permitted under this clause.

(ii) Professional and technical services.

(A) The prohibition on the use of appropriated funds, in subparagraph (b)(1) of this clause, does not apply in the case of--

(1) A payment of reasonable compensation made to an officer or employee of a person requesting or receiving a covered Federal action or an extension, continuation, renewal, amendment, or modification of a covered Federal action, if payment is for professional or technical services rendered directly in the preparation, submission, or negotiation of any bid, proposal, or application for that Federal action or for meeting requirements imposed by or pursuant to law as a condition for receiving that Federal action.

(2) Any reasonable payment to a person, other than an officer or employee of a person requesting or receiving a covered Federal action or an extension, continuation, renewal, amendment, or modification of a covered Federal action if the payment is for professional or technical services rendered directly in the preparation, submission, or negotiation of any bid, proposal, or application for that Federal action or for meeting requirements imposed by or pursuant to law as a condition for receiving that Federal action. Persons other than officers or employees of a person requesting or receiving a covered Federal action include consultants and trade associations.

(B) For purposes of subdivision (b)(3)(ii)(A) of this clause, "professional and technical services" shall be limited to advice and analysis directly applying any professional or technical discipline. For example, drafting of a legal document accompanying a bid or proposal by a lawyer is allowable. Similarly, technical advice provided by an engineer on the performance or operational capability of a piece of equipment rendered directly in the negotiation of a contract is allowable. However, communications with the intent to 'nfluence made by a professional (such as a licensed lawyer) or a technical person (such as a licensed accountant) are not allowable under this section unless they provide advice and analysis directly applying their professional or technical expertise and unless the advice or analysis is rendered directly and solely in the preparation, submission or negotiation of a covered Federal action. Thus, for example, communications with the intent to influence made by a lawyer that do not provide legal advice or analysis directly and solely related to the legal aspects of his or her client's proposal, but generally advocate one proposal over another are not allowable under this section because the lawyer is not providing professional legal services. Similarly, communications with the intent to influence made by an engineer providing an engineering analysis prior to the preparation or submission of a bid or proposal are not allowable under this section since the engineer is providing technical services but not directly in the preparation, submission or negotiation of a covered Federal action.

(C) Requirements imposed by or pursuant to law as a condition for receiving a covered Federal award include those required by law or regulation and any other requirements in the actual award documents.

(D) Only those services expressly authorized by subdivisions (b)(3)(ii)(A)(1) and (2) of this clause are permitted under this clause.

(E) The reporting requirements of FAR 3.803(a) shall not apply with respect to payments of reasonable compensation made to regularly employed officers or employees of a person.

(c) Disclosure.

(1) The Contractor who requests or receives from an agency a Federal contract shall file with that agency a disclosure form, OMB standard form LLL, Disclosure of Lobbying Activities, if such person has made or has agreed to make any payment using nonappropriated funds (to include profits from any covered Federal action), which would be prohibited under subparagraph (b)(1) of this clause, if paid for with appropriated funds.

(2) The Contractor shall file a disclosure form at the end of each calendar quarter in which there occurs any event that materially affects the accuracy of the information contained in any disclosure form previously filed by such person under subparagraph (c)(1) of this clause. An event that materially affects the accuracy of the information reported includes—

(i) A cumulative increase of $25,000 or more in the amount paid or expected to be paid for influencing or attempting to influence a covered Federal action; or

(ii) A change in the person(s) or individual(s) influencing or attempting to influence a covered Federal action; or

(iii) A change in the officer(s), employee(s), or Member(s) contacted to influence or attempt to influence a covered Federal action.

(3) The Contractor shall require the submittal of a certification, and if required, a disclosure form by any person who requests or receives any subcontract exceeding $100,000 under the Federal contract.

(4) All subcontractor disclosure forms (but not certifications) shall be forwarded from tier to tier until received by the prime Contractor. The prime Contractor shall submit all disclosures to the Contracting Officer at the end of the calendar quarter in which the disclosure form is submitted by the subcontractor. Each subcontractor certification shall be retained in the subcontract file of the awarding Contractor.

(d) Agreement. The Contractor agrees not to make any payment prohibited by this clause.

(e) Penalties.

(1) Any person who makes an expenditure prohibited under paragraph (a) of this clause or who fails to file or amend the disclosure form to be filed or amended by paragraph (b) of this clause shall be subject to civil penalties as provided for by 31 U.S.C. 1352. An imposition of a civil penalty does not prevent the Government from seeking any other remedy that may be applicable.

(2) Contractors may rely without liability on the representation made by their subcontractors in the certification and disclosure form.

(f) Cost allowability. Nothing in this clause makes allowable or reasonable any costs which would otherwise be unallowable or unreasonable. Conversely, costs made specifically unallowable by the requirements in this clause will not be made allowable under any other provision.

I.5 52.244-2 SUBCONTRACTS (AUG 1998)

(a) *Definitions.* As used in this clause-
"Approved purchasing system" means a Contractor's purchasing system that has been reviewed and approved in accordance with Part 44 of the Federal Acquisition Regulation (FAR).
"Consent to subcontract" means the Contracting Officer's written consent for the Contractor to enter into a particular subcontract.
"Subcontract" means any contract, as defined in FAR Subpart 2.1, entered into by a subcontractor to furnish supplies or services for performance of the prime contract or a subcontract. It includes, but is not limited to, purchase orders, and changes and modifications to purchase orders.
(b) This clause does not apply to subcontracts for special test equipment when the contract contains the clause at FAR 52.245-18, Special Test Equipment.
(c) When this clause is included in a fixed-price type contract, consent to subcontract is required only on unpriced contract actions (including unpriced modifications or unpriced delivery orders), and only if required in accordance with paragraph (d) or (e) of this clause.
(d) If the Contractor does not have an approved purchasing system, consent to subcontract is required for any subcontract that-
(1) Is of the cost-reimbursement, time-and-materials, or labor-hour type; or
(2) Is fixed-price and exceeds-
(i) For a contract awarded by the Department of Defense, the Coast Guard, or the National Aeronautics and Space Administration, the greater of the simplified acquisition threshold or 5 percent of the total estimated cost of the contract; or
(ii) For a contract awarded by a civilian agency other than the Coast Guard and the National Aeronautics and Space Administration, either the simplified acquisition threshold or 5 percent of the total estimated cost of the contract.
(e) If the Contractor has an approved purchasing system, the Contractor nevertheless shall obtain the Contracting Officer's written consent before placing the following subcontracts:

____

____

____

(f) (1) The Contractor shall notify the Contracting Officer reasonably in advance of placing any subcontract or modification thereof for which consent is required under paragraph (c), (d), or (e) of this clause, including the following information:
(i) A description of the supplies or services to be subcontracted.
(ii) Identification of the type of subcontract to be used.
(iii) Identification of the proposed subcontractor.
(iv) The proposed subcontract price.
(v) The subcontractor's current, complete, and accurate cost or pricing data and Certificate of Current Cost or Pricing Data, if required by other contract provisions.
(vi) The subcontractor's Disclosure Statement or Certificate relating to Cost Accounting Standards when such data are required by other provisions of this contract.
(vii) A negotiation memorandum reflecting-
(A) The principal elements of the subcontract price negotiations;
(B) The most significant considerations controlling establishment of initial or revised prices;
(C) The reason cost or pricing data were or were not required;
(D) The extent, if any, to which the Contractor did not rely on the subcontractor's cost or pricing data in determining the price objective and in negotiating the final price;
(E) The extent to which it was recognized in the negotiation that the subcontractor's cost or pricing data were not accurate, complete, or current; the action taken by the Contractor and the subcontractor; and the effect of any such defective data on the total price negotiated;
(F) The reasons for any significant difference between the Contractor's price objective and the price negotiated; and
(G) A complete explanation of the incentive fee or profit plan when incentives are used. The explanation shall identify each critical performance element, management decisions used to quantify each incentive element, reasons for the incentives, and a summary of all trade-off possibilities considered.

(2) The Contractor is not required to notify the Contracting Officer in advance of entering into any subcontract for which consent is not required under paragraph (c), (d), or (e) of this clause.
(g) Unless the consent or approval specifically provides otherwise, neither consent by the Contracting Officer to any subcontract nor approval of the Contractor's purchasing system shall constitute a determination-
(1) Of the acceptability of any subcontract terms or conditions;
(2) Of the allowability of any cost under this contract; or
(3) To relieve the Contractor of any responsibility for performing this contract.
(h) No subcontract or modification thereof placed under this contract shall provide for payment on a cost-plus-a-percentage-of-cost basis, and any fee payable under cost-reimbursement type subcontracts shall not exceed the fee limitations in FAR 15.404-4(c)(4)(i).
(i) The Contractor shall give the Contracting Officer immediate written notice of any action or suit filed and prompt notice of any claim made against the Contractor by any subcontractor or vendor that, in the opinion of the Contractor, may result in litigation related in any way to this contract, with respect to which the Contractor may be entitled to reimbursement from the Government.
(j) The Government reserves the right to review the Contractor's purchasing system as set forth in FAR Subpart 44.3.
(k) Paragraphs (d) and (f) of this clause do not apply to the following subcontracts, which were evaluated during negotiations

____

____

____

I.6 52.219-06 NOTICE OF TOTAL SMALL BUSINESS SET-ASIDE JUNE 2003

(a) Definition. "Small business concern," as used in this clause, means a concern, including its affiliates, that is independently owned and operated, not dominant in the field of operation in which it is bidding on Government contracts, and qualified as a small business under the size standards in this solicitation.
(b) General.

(1) Offers are solicited only from small business concerns. Offers received from concerns that are not small business concerns shall be considered nonresponsive and will be rejected.
(2) Any award resulting from this solicitation will be made to a small business concern.
(a) Agreement. A small business concern submitting an offer in its own name shall furnish, in performing the contract, only end items manufactured or produced by small business concerns in the United States or its outlying areas. If this procurement is processed under simplified acquisition procedures and the total amount of this contract does not exceed $25,000, a small business concern may furnish the product of any domestic firm. This paragraph does not apply to construction or service contracts.

I.7 52.244-06 SUBCONTRACTS FOR COMMERCIAL ITEMS MAY 2002

(a) Definitions. As used in this clause-

"Commercial item" has the meaning contained in the clause at 52.202-1, Definitions.

"Subcontract" includes a transfer of commercial items between divisions, subsidiaries, or affiliates of the Contractor or subcontractor at any tier.

(b) To the maximum extent practicable, the Contractor shall incorporate, and require its subcontractors at all tiers to incorporate, commercial items or nondevelopmental items as components of items to be supplied under this contract.

(c)(1) The Contractor shall insert the following clauses in subcontracts for commercial items:

(i) 52.219-8, Utilization of Small Business Concerns (OCT 2000) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds $500,000 ($1,000,000 for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(ii) 52.222-26, Equal Opportunity (APR 2002) (E.O. 11246).

(iii) 52.222-35, Equal Opportunity for Special Disabled Veterans, Veterans of the Vietnam Era, and Other Eligible Veterans (DEC 2001) (38 U.S.C. 4212(a)).

(iv) 52.222-36, Affirmative Action for Workers with Disabilities (JUN 1998) (29 U.S.C. 793).

(v) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (JUN 2000) (46 U.S.C. Appx 1241) (flowdown not required for subcontracts awarded beginning May 1, 1996).

(2) While not required, the Contractor may flow down to subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

(d) The Contractor shall include the terms of this clause, including this paragraph (d), in subcontracts awarded under this contract.

I.8 52.204-7 CENTRAL CONTRACTOR REGISTRATION (OCT 2003)

(a) Definitions. As used in this clause-
"Central Contractor Registration (CCR) database" means the primary Government repository for Contractor information required for the conduct of business with the Government.
"Data Universal Numbering System (DUNS) number" means the 9-digit number assigned by Dun and Bradstreet, Inc. (D&B) to identify unique business entities.
"Data Universal Numbering System +4 (DUNS+4) number" means the DUNS number assigned by D&B plus a 4-character suffix that may be assigned by a business concern. (D&B has no affiliation with this 4-character suffix.) This 4-character suffix may be assigned at the discretion of the business concern to establish additional CCR records for identifying alternative Electronic Funds Transfer (EFT) accounts (see the FAR at Subpart 32.11) for the same parent concern.
"Registered in the CCR database" means that-
(1) The Contractor has entered all mandatory information, including the DUNS number or the DUNS+4 number, into the CCR database; and
(2) The Government has validated all mandatory data fields and has marked the record "Active".
(b)(1) By submission of an offer, the offeror acknowledges the requirement that a prospective awardee shall be registered in the CCR database prior to award, during performance, and through final payment of any contract, basic agreement, basic ordering agreement, or blanket purchasing agreement resulting from this solicitation.
(2) The offeror shall enter, in the block with its name and address on the cover page of its offer, the annotation "DUNS" or "DUNS +4" followed by the DUNS or DUNS +4 number that identifies the offeror's name and address exactly as stated in the offer. The DUNS number will be used by the Contracting Officer to verify that the offeror is registered in the CCR database.
(c) If the offeror does not have a DUNS number, it should contact Dun and Bradstreet directly to obtain one.
(1) An offeror may obtain a DUNS number-
(i) If located within the United States, by calling Dun and Bradstreet at 1-866-705-5711 or via the Internet at *http://www.dnb.com*; or
(ii) If located outside the United States, by contacting the local Dun and Bradstreet office.
(2) The offeror should be prepared to provide the following information:
(i) Company legal business.
(ii) Tradestyle, doing business, or other name by which your entity is commonly recognized.
(iii) Company Physical Street Address, City, State, and Zip Code.
(iv) Company Mailing Address, City, State and Zip Code (if separate from physical).
(v) Company Telephone Number.
(vi) Date the company was started.
(vii) Number of employees at your location.
(viii) Chief executive officer/key manager.

(ix) Line of business (industry).
(x) Company Headquarters name and address (reporting relationship within your entity).
(d) If the Offeror does not become registered in the CCR database in the time prescribed by the Contracting Officer, the Contracting Officer will proceed to award to the next otherwise successful registered Offeror.
(e) Processing time, which normally takes 48 hours, should be taken into consideration when registering. Offerors who are not registered should consider applying for registration immediately upon receipt of this solicitation.
(f) The Contractor is responsible for the accuracy and completeness of the data within the CCR database, and for any liability resulting from the Government's reliance on inaccurate or incomplete data. To remain registered in the CCR database after the initial registration, the Contractor is required to review and update on an annual basis from the date of initial registration or subsequent updates its information in the CCR database to ensure it is current, accurate and complete. Updating information in the CCR does not alter the terms and conditions of this contract and is not a substitute for a properly executed contractual document.
(g) (1) (i) If a Contractor has legally changed its business name, "doing business as" name, or division name (whichever is shown on the contract), or has transferred the assets used in performing the contract, but has not completed the necessary requirements regarding novation and change-of-name agreements in Subpart 42.12, the Contractor shall provide the responsible Contracting Officer a minimum of one business day's written notification of its intention to (A) change the name in the CCR database; (B) comply with the requirements of Subpart 42.12 of the FAR; and (C) agree in writing to the timeline and procedures specified by the responsible Contracting Officer. The Contractor must provide with the notification sufficient documentation to support the legally changed name.
(ii) If the Contractor fails to comply with the requirements of paragraph (g)(1)(i) of this clause, or fails to perform the agreement at paragraph (g)(1)(i)(C) of this clause, and, in the absence of a properly executed novation or change-of-name agreement, the CCR information that shows the Contractor to be other than the Contractor indicated in the contract will be considered to be incorrect information within the meaning of the "Suspension of Payment" paragraph of the electronic funds transfer (EFT) clause of this contract.
(2) The Contractor shall not change the name or address for EFT payments or manual payments, as appropriate, in the CCR record to reflect an assignee for the purpose of assignment of claims (see FAR Subpart 32.8, Assignment of Claims). Assignees shall be separately registered in the CCR database. Information provided to the Contractor's CCR record that indicates payments, including those made by EFT, to an ultimate recipient other than that Contractor will be considered to be incorrect information within the meaning of the "Suspension of payment" paragraph of the EFT clause of this contract.
(h) Offerors and Contractors may obtain information on registration and annual confirmation requirements via the internet at *http://www.ccr.gov* or by calling 1-888-227-2423, or 269-961-5757.

SECTION J – LIST OF ATTACHMENTS

Attachment 1 – Instructions for Monthly Status Report

Attachment 2 – Sample Cost Status Sheet (Monthly Status Report)

Attachment 3 – Generalized Markup Language /eXtensible Markup Language /Resource Management

Attachment 4 – Instructions for Resource Estimate

Attachment 5 – Sample Sheet 1 (Resource Estimate)

Attachment 6 – Sample Sheet 2 (Resource Estimate)

Attachment 7 – Data Quality Management Guide

Attachment 8 – Technical Standard and Guideline Data Element Standardization

Attachment 9 – Technical Standard and Guideline Data Management

Attachment 10 – Life Cycle Management

SECTION K -- REPRESENTATIONS, CERTIFICATIONS AND OTHER STATEMENTS OF OFFERORS

.1 52.252-01 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. The offeror is cautioned that the listed provisions may include blocks that must be completed by the offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation or offer. Also, the full text of a solicitation provision may be accessed electronically at this/these address(es):

http://www.arnet.gov/far/loadindex.html ---------------------

----

Clause	Title	Date
52.222-38	Compliance with Veterans' Employment Reporting Requirements	December 2001

K.2 52.203-02 CERTIFICATE OF INDEPENDENT PRICE DETERMINATION APRIL 1985

(a) The offeror certifies that -

(1) The prices in this offer have been arrived at independently, without, for the purpose of restricting competition, any consultation, communication, or agreement with any other offeror or competitor relating to
(i) those prices,
(ii) the intention to submit an offer, or
(iii) the methods of factors used to calculate the prices offered:

(2) The prices in this offer have not been and will not be knowingly disclosed by the offeror, directly or indirectly, to any other offeror or competitor before bid opening (in the case of a sealed bid solicitation) or contract award (in the case of a negotiated solicitation) unless otherwise required by law; and

(3) No attempt has been made or will be made by the offeror to induce any other concern to submit or not to submit an offer for the purpose of restricting competition.

(b) Each signature on the offer is considered to be a certification by the signatory that the signatory -

(1) Is the person in the offeror's organization responsible for determining the prices offered in this bid or proposal, and that the signatory has not participated and will not participate in any action contradictory to subparagraphs (a)(1) through (a)(3) of this provision; or

(2) (i) Has been authorized, in writing, to act as an agent for the following principals in certifying that those principals have not participated, and will not participate in any action contrary to subparagraphs (a)(1) through (a)(3) of this provision (insert full name of person(s) in the offeror's organization responsible for determining the prices offered in this bid or proposal, and the title of his or her position in the offeror's organization);

(ii) As an authorized agent, does certify that the principals named in subdivision (b)(2)(i) of this provision have not participated, and will not participate, in any action contrary to subparagraphs (a)(1) through (a)(3) of this provision; and

ii) As an agent, has not personally participated, and will not participate, in any action contrary to subparagraphs (a)(1) through (a)(3) of this rovision.

(c) If the offeror deletes or modifies subparagraph (a)(2) of this provision, the offeror must furnish with its offer a signed statement setting forth in detail the circumstances of the disclosure.

K.3 52.203-11 CERTIFICATION AND DISCLOSURE REGARDING PAYMENT TO INFLUENCE CERTAIN FEDERAL TRANSACTIONS APRIL 1991

(a) The definitions and prohibitions contained in the clause, at FAR 52.203-12, Limitation on Payments to Influence Certain Federal Transactions, included in this solicitation, are hereby incorporated by reference in paragraph (b) of this Certification.

(b) The offeror, by signing its offer, hereby certifies to the best of his or her knowledge and belief that on or after December 23, 1989,

(1) No Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a member of Congress on his or her behalf in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment or modification of any Federal contract, grant, loan, or cooperative agreement;

(2) If any funds other than Federal appropriated funds (including profit or fee received under a covered Federal transaction) have been paid, or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress or an employee of a Member of Congress on his or her behalf in connection with this solicitation, the offeror shall complete and submit, with its offer, OMB standard form LLL, Disclosure of Lobbying Activities, to the Contracting Officer; and

) He or she will include the language of this certification in all subcontract awards at any tier and require that all recipients of subcontract awards in excess of $100,000 shall certify and disclose accordingly.

(c) Submission of this certification and disclosure is a prerequisite for making or entering into this contract imposed by section 1352, title 31, United States Code. Any person who makes an expenditure prohibited under this provision, shall be subject to a civil penalty of not less than $10,000, and not more than $100,000, for each such failure.

K.4 52.204-03 TAXPAYER IDENTIFICATION OCTOBER 1998

(a) Definitions.

"Common parent," as used in this provision, means that corporate entity that owns or controls an affiliated group of corporations that files its Federal income tax returns on a consolidated basis, and of which the offeror is a member.

"Taxpayer Identification Number (TIN)," as used in this provision, means the number required by the Internal Revenue Service (IRS) to be used by the offeror in reporting income tax and other returns. The TIN may be either a Social Security Number or an Employer Identification Number.

(b) All offerors must submit the information required in paragraphs (d) through (f) of this provision to comply with debt collection requirements of 31 U.S.C. 7701(c) and 3325(d), reporting requirements of 26 U.S.C. 6041, 6041A, and 6050M, and implementing regulations issued by the IRS. If the resulting contract is subject to the payment reporting requirements described in Federal Acquisition Regulation (FAR) ·904, the failure or refusal by the offeror to furnish the information may result in a 31 percent reduction ı payments otherwise due under the contract.

(c) The TIN may be used by the Government to collect and report on any delinquent amounts arising out of the offeror's relationship with the Government (31 U.S.C. 7701(c)(3)). If the resulting contract is subject to the payment reporting requirements described in FAR 4.904, the TIN provided hereunder may be matched with IRS records to verify the accuracy of the offeror's TIN.

(d) Taxpayer Identification Number (TIN).

[ ] TIN:
59-3176720 .

[ ] TIN has been applied for.

[ ] TIN is not required because:

[ ] Offeror is a nonresident alien, foreign corporation, or foreign partnership that does not have income effectively connected with the conduct of a trade or business in the United States and does not have an office or place of business or a fiscal paying agent in the United States;

[ ] Offeror is an agency or instrumentality of a foreign government;
[ ] Offeror is an agency or instrumentality of the Federal Government. (e)

Type of organization.

[ ] Sole proprietorship;

, Partnership;

[x] Corporate entity (not tax-exempt);

[ ] Corporate entity (tax-exempt);

[ ] Government entity (Federal, State, or local);

[ ] Foreign government;

[ ] International organization per 26 CFR 1.6049-4;

[ ] Other
______________________.

(f) Common parent.

[ ] Offeror is not owned or controlled by a common parent as defined in paragraph (a) of this provision.

[ ] Name and TIN of common parent:

Name
____

TIN

____

K.5 52.204-05 WOMEN-OWNED BUSINESS (OTHER THAN SMALL BUSINESS) MAY 1999

(a) Definition. "Women-owned business concern," as used in this provision, means a concern that is at least 51 percent owned by one or more women; or in the case of any publicly owned business, at least 51 percent of its stock is owned by one or more women; and whose management and daily business operations are controlled by one or more women.

(b) Representation. [Complete only if the offeror is a women-owned business concern and has not represented itself as a small business concern in paragraph (b)(1) of FAR 52.219-1, Small Business Program Representations, of this solicitation.] The offeror represents that it ( ) is a women-owned business concern.

K.6 52.209-05 CERTIFICATION REGARDING DEBARMENT, SUSPENSION, PROPOSED DEBARMENT, AND OTHER RESPONSIBILITY MATTERS DECEMBER 2001

(a)(1) The Offeror certifies, to the best of its knowledge and belief, that-(i) The

Offeror and/or any of its Principals-

(A) Are [ ] are not [x] presently debarred, suspended, proposed for debarment, or declared ineligible for the award of contracts by any Federal agency;

(B) Have [ ] have not [x], within a three-year period preceding this offer, been convicted of or had a civil judgment rendered against them for: mmission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, state, or local) contract or subcontract; violation of Federal or state antitrust statutes relating to the submission of offers; or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, or receiving stolen property; and

(C) Are [ ] are not [x] presently indicted for, or otherwise criminally or civilly charged by a governmental entity with, commission of any of the offenses enumerated in paragraph (a)(1)(i)(B) of this provision.

(ii) The Offeror has [ ] has not [x], within a three-year period preceding this offer, had one or more contracts terminated for default by any Federal agency.

(2) "Principals," for the purposes of this certification, means officers; directors; owners; partners; and, persons having primary management or supervisory responsibilities within a business entity (e.g., general manager; plant manager; head of a subsidiary, division, or business segment, and similar positions).

THIS CERTIFICATION CONCERNS A MATTER WITHIN THE JURISDICTION OF AN AGENCY OF THE UNITED STATES AND THE MAKING OF A FALSE, FICTITIOUS, OR FRAUDULENT CERTIFICATION MAY RENDER THE MAKER SUBJECT TO PROSECUTION UNDER SECTION 1001, TITLE 18, UNITED STATES CODE.

(b) The Offeror shall provide immediate written notice to the Contracting Officer if, at any time prior to contract award, the Offeror learns that its certification was erroneous when submitted or has become erroneous by reason of changed circumstances.

(c) A certification that any of the items in paragraph (a) of this provision exists will not necessarily result in withholding of an award under this solicitation. However, the certification will be considered in connection with a determination of the Offeror's responsibility. Failure of the Offeror to furnish a certification or provide such additional information as requested by the Contracting Officer may render the Offeror nonresponsible.

(d) Nothing contained in the foregoing shall be construed to require establishment of a system of records in order to render, in good faith, the certification required by paragraph (a) of this provision. The knowledge and information of an Offeror is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.

(e) The certification in paragraph (a) of this provision is a material representation of fact upon which reliance was placed when making award. If it is later determined that the Offeror knowingly rendered an erroneous certification, in addition to other remedies available to the Government, the Contracting Officer may terminate the contract resulting from this solicitation for default.

K.7 52.215-06 PLACE OF PERFORMANCE OCTOBER 1997

(a) The offeror or respondent, in the performance of any contract resulting from this solicitation, [x] intends, _ does not intend [check applicable block] to use one or more plants or facilities located at a different address from the address of the offeror or respondent as indicated in this proposal or response to request for information.

(b) If the offeror or respondent checks ``intends" in paragraph (a) of this provision, it shall insert in the following spaces the required information:

Place of Performance Name and Address of Owner
(Street Address, City, and Operator of the Plant
State, County, Zip Code) or Facility if Other than Offeror or Respondent

Three Crystal Park
2231 Crystal Drive, Suite 800
Arlington, VA 22202

Galaxy Scientific Corporation
3120 Fire Road
Egg Harbor Township, NJ 08234

K.8 52.215-07 ANNUAL REPRESENTATIONS AND CERTIFICATIONS-- OCTOBER 1997 NEGOTIATION

The offeror has [check the appropriate block]:

(a) Submitted to the contracting office issuing this solicitation, annual representations and certifications dated ------------------[insert date of signature on submission] that are incorporated herein by reference, and are current, accurate, and complete as of the date of this proposal, except as follows [insert changes that affect only this proposal; if ``none," so state]:

___x___(b) Enclosed its annual representations and certifications.

K.9 52.219-01 SMALL BUSINESS PROGRAM REPRESENTATIONS APRIL 2002

(a)(1) The North American Industry Classification System (NAICS) code for this acquisition is 541519.

(2) The small business size standard is **$21 million annually.**

(3) The small business size standard for a concern which submits an offer in its own name, other than on a construction or service contract, but which proposes to furnish a product which it did not itself manufacture, is 500 employees.

(b) Representations. (1) The offeror represents as part of its offer that it [x] is _ is not a small business concern.

(2) [Complete only if the offeror represented itself as a small business concern in paragraph (b)(1) of this provision.] The offeror represents, for general statistical purposes, that it [x] is, is not, a small disadvantaged business concern as defined in 13 CFR 124.1002.

') [Complete only if the offeror represented itself as a small business concern in paragraph (b)(1) of this provision.] The offeror represents as ,art of its offer that it is, [x] is not a women-owned small business concern.

(4) [Complete only if the offeror represented itself as a small business concern in paragraph (b)(1) of this provision.] The offeror represents as part of its offer that it is, [x] is not a veteran-owned small business concern.

(5) [Complete only if the offeror represented itself as a veteran-owned small business concern in paragraph (b)(4) of this provision.] The offeror represents as part of its offer that it is, [x] is not a service-disabled veteran-owned small business concern.

(6) [Complete only if the offeror represented itself as a small business concern in paragraph (b)(1) of this provision.] The offeror represents, as part of its offer, that—

(i) It [ ] is, [x] is not a HUBZone small business concern listed, on the date of this representation, on the List of Qualified HUBZone Small Business Concerns maintained by the Small Business Administration, and no material change in ownership and control, principal office, or HUBZone employee percentage has occurred since it was certified by the Small Business Administration in accordance with 13 CFR part 126; and

(ii) It [ ] is, [x] is not a joint venture that complies with the requirements of 13 CFR part 126, and the representation in paragraph (b)(6)(i) of this provision is accurate for the HUBZone small business concern or concerns that are participating in the joint venture. [The offeror shall enter the name or names of the HUBZone small business concern or concerns that are participating in the joint venture: .] Each HUBZone small business concern participating in the joint venture shall submit a separate signed copy of the HUBZone representation.

(c) Definitions. As used in this provision-"Service-disabled

veteran-owned small business concern"-(1) Means a small

business concern-

.) Not less than 51 percent of which is owned by one or more service-disabled veterans or, in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more service-disabled veterans; and

(ii) The management and daily business operations of which are controlled by one or more service-disabled veterans or, in the case of a veteran with permanent and severe disability, the spouse or permanent caregiver of such veteran.

(2) Service-disabled veteran means a veteran, as defined in 38 U.S.C. 101(2), with a disability that is service-connected, as defined in 38 U.S.C. 101(16).

"Small business concern" means a concern, including its affiliates, that is independently owned and operated, not dominant in the field of operation in which it is bidding on Government contracts, and qualified as a small business under the criteria in 13 CFR part 121 and the size standard in paragraph (a) of this provision.

"Veteran-owned small business concern" means a small business concern-

(1) Not less than 51 percent of which is owned by one or more veterans (as defined at 38 U.S.C. 101(2)) or, in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more veterans; and

(2) The management and daily business operations of which are controlled by one or more veterans. "Women-

owned small business concern" means a small business concern-

(1) That is at least 51 percent owned by one or more women; or, in the case of any publicly owned business, at least 51 percent of the stock of which is owned by one or more women; and

(2) Whose management and daily business operations are controlled by one or more women.

(d) Notice. (1) If this solicitation is for supplies and has been set aside, in whole or in part, for small business concerns, then the clause in this solicitation providing notice of the set-aside contains restrictions on the source of the end items to be furnished.

.2) Under 15 U.S.C. 645(d), any person who misrepresents a firm's status as a small, HUBZone small, small disadvantaged, or womenowned small business concern in order to obtain a contract to be awarded under the preference programs established pursuant to section 8(a), 8(d), 9, or 15 of the Small Business Act or any other provision of Federal law that specifically references section 8(d) for a definition of program eligibility, shall-

(i) Be punished by imposition of fine, imprisonment, or both;

(ii) Be subject to administrative remedies, including suspension and debarment; and

(iii) Be ineligible for participation in programs conducted under the authority of the Act.

K.10 52.222-22 PREVIOUS CONTRACTS AND COMPLIANCE REPORTS FEBRUARY 1999

The offeror represents that-

(a) It [ ] has, [x] has not participated in a previous contract or subcontract subject to the Equal Opportunity clause of this solicitation;

(b) It [x] has [ ] has not filed all required compliance reports; and

(c) Representations indicating submission of required compliance reports, signed by proposed subcontractors, will be obtained before subcontract awards.

..11 52.222-25 AFFIRMATIVE ACTION COMPLIANCE APRIL 1984

The offeror represents that (a) [x] it has developed and has on file, [ ] has not developed and does not have on file, at each establishment, affirmative action programs required by the rules and regulations of the Secretary of Labor (41 CFR 60-1 and 60-2), or (b) [ ] has not previously had contracts subject to the written affirmative action programs requirement of the rules and regulations of the Secretary of Labor.

K.12 52.223-13 CERTIFICATION OF TOXIC CHEMICAL RELEASE REPORTING OCTOBER 2000

(a) Submission of this certification is a prerequisite for making or entering into this contract imposed by Executive Order 12969, August 8, 1995.

(b) By signing this offer, the offeror certifies that-

(1) As the owner or operator of facilities that will be used in the performance of this contract that are subject to the filing and reporting requirements described in section 313 of the Emergency Planning and Community Right-to-Know Act of 1986 (EPCRA) (42 U.S.C. 11023) and section

6607 of the Pollution Prevention Act of 1990 (PPA) (42 U.S.C. 13106), the offeror will file and continue to file for such facilities for the life of the contract the Toxic Chemical Release Inventory Form (Form R) as described in sections 313(a) and (g) of EPCRA and section 6607 of PPA; or

_) None of its owned or operated facilities to be used in the performance of this contract is subject to the Form R filing and reporting requirements because each such facility is exempt for at least one of the following reasons: [Check each block that is applicable.]

[x] (i) The facility does not manufacture, process, or otherwise use any toxic chemicals listed under section 313(c) of EPCRA, 42 U.S.C. 11023(c);

[ ] (ii) The facility does not have 10 or more full-time employees as specified in section 313(b)(1)(A) of EPCRA, 42 U.S.C. 11023(b)(1)(A);

[ ] (iii) The facility does not meet the reporting thresholds of toxic chemicals established under section 313(f) of EPCRA, 42 U.S.C. 11023(f) (including the alternate thresholds at 40 CFR 372.27, provided an appropriate certification form has been filed with EPA);

[ ] (iv) The facility does not fall within Standard Industrial Classification Code (SIC) designations 20 through 39 as set forth in section 19.102 of the Federal Acquisition Regulation; or

[ ] (v) The facility is not located within any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, Guam, American Samoa, the United States Virgin Islands, the Northern Mariana Islands, or any other territory or possession over which the United States has jurisdiction.

(a) The offeror, by signing this offer, certifies that -

_x_ (1) To the best of its knowledge and belief, it is not subject to the filing and reporting requirements described in Emergency Planning and Community Right-to-Know Act of 1986 (EPCRA) sections 313(a) and (g) and Pollution Prevention Act (PPA) section 6607 because none of its owned or operated facilities to be used in the performance of this contract currently -

_ (i) Manufacture, process or otherwise use any toxic chemicals listed under section 313(c) of EPCRA, 42 U.S.C. 11023(c).

___ (ii) Have more than 10 or more full-time employees as specified in section 313(b)(1)(A) of EPCRA, 42 U.S.C. 11023(b)(1)(A).

___ (iii) Meet the reporting thresholds in toxic chemicals established under section 313(f) of EPCRA, 42 U.S.C. 11023(f) (including the alternate thresholds at 40 CFR 372.27, provided an appropriate certification form has been filed with EPA).

___ (iv) Fall within Standard Industrial Classification Code (SIC) designations 20 through 39 as set forth in FAR section 19.102.

___ (2) If awarded a contract resulting from this solicitation, its owned or operated facilities to be used in the performance of this contract, unless otherwise exempt, will file and continue to file for the life of the contract the Toxic Chemical Release Inventory Form (Form R) as described in EPCRA sections 313(a) and (g) and PPA section 6607 (42 U.S.C. 13106).

(b) Submission of this certification is a prerequisite for making or entering into this contract imposed by Executive order 12969, August 8, 1995 (60 FR 40989-40992).

K.13 CERTIFICATION

I hereby certify that the responses to the above Representations, Certifications and other statements are accurate and complete.

Signature: ____________________

Title: Chief Operating Officer

Date: 10/08/2003

SECTION J – LIST OF ATTACHMENTS

Attachment 1 – Instructions for Monthly Status Report

Attachment 2 – Sample Cost Status Sheet (Monthly Status Report)

Attachment 3 – Generalized Markup Language /eXtensible Markup Language /Resource Management

Attachment 4 – Instructions for Resource Estimate

Attachment 5 – Sample Sheet 1 (Resource Estimate)

Attachment 6 – Sample Sheet 2 (Resource Estimate)

Attachment 7 – Data Quality Management Guide

Attachment 8 – Technical Standard and Guideline Data Element Standardization

Attachment 9 – Technical Standard and Guideline Data Management

Attachment 10 – Life Cycle Management

Attachment 1

Instructions for FN01, Monthly Status Report

Deliverable Number: FN01

Title/Description: Monthly Status Report

Frequency of Submission: Monthly

No. of Copies: 5

Submission is Due: Due 18th day of the month following the end of the reporting month.

Government Assistance Required: Yes

Government Response Due: 10 working days after receipt.

Format/Content Requirements and Instructions: This report is prepared by the contractor to provide a comprehensive review and analysis of cost, schedule, and technical performance of each contract task. Status report data will be used by USPTO management to: (1) evaluate task performance; (2) identify the magnitude and impact of actual and potential problem areas causing significant cost and schedule variances from plan; and (3) provide valid, timely, and auditable task order status information to USPTO executive management.

Application/Interrelationship: Data reported in the Monthly Status Report will pertain to all authorized tasks. The level of detail to be reported normally will be limited to Task Orders. If no specific Task Order specific variance is specified, cost variance analysis and explanation will be provided at the task order level if the current month actual cost variance is more than (+/-) 10% of the planned budget unless the collar variance is within (+/-) $2,500 of the planned budget or if the cumulative variance is more than (+/-) 10% of planned budget unless the dollar variance is within (+/-) $10,000 of the planned budget.

Preparation Instructions: The Monthly Status Report shall be submitted in accordance with the following format requirements:

Section 1 Executive Summary
Section 2 Active Task Order Status
For each task order the following will be provided:
--Task Order Summary
--Task Status
--Outlook for Next Month
Appendix A--Hours by Task and Individual Name

Section 1--Executive Summary: The contractor shall provide a brief narrative of the accomplishments, problems, and issues regarding all formally authorized tasks. This section should reflect the contractor's assessment of overall task status (cost, schedule, and technical) in relation to planned performance. Schedule performance should be discussed in terms of the key milestones associated with the task orders. Monthly and cumulative budget vs. actual cost and cost variance shall be provided at the task order level.

In addition, the contractor shall report on the monthly status of the task order development and implementation process in accordance with the following:

Task Orders in process (by title, budget value, and period of performance)
Task Orders under development (by title, status, and PTO point of contact)
Task Orders completed during month (by Title and completion date)

Section 2--Active Task Order Status: Cost and technical status will be reported at the task order level unless specified in the task order.

Cost Status (see sample)--
A cost summary will be provided at the task order level that depicts the following:

Current and cumulative budgeted hours direct labor hours by labor Category

Current and cumulative actual direct labor hours expended on the task Order by labor category.

Current and cumulative variances between budgeted and actual labor Hours by labor category.

Current and cumulative budgeted and actual subcontractor labor hours By labor category.

Current and cumulative budgeted and other actual costs (if any).

Task Order budget at completion.

Task Order estimate at completion and variance at completion. The Frequency of providing a revised estimate at completion will be Subject to negotiation between PTO and the contractor.

Technical Status: Technical status will be reported in terms of objectives established in the Task order. The contractor shall, whenever possible, establish objective criteria for evaluating technical progress in relation to the plan for accomplishing the technical objectives of the contract.

Variance Analysis: Variance analysis shall include:

Nature of the variance (dollars/percentage over or under budget)
Reason(s) for the variance

Impact on the task order

Corrective action taken

Outlook for Next Month: This section will contain a compilation of all significant activities and events to be addressed in the next monthly status report. The contractor will specifically address workarounds and other planning efforts undertaken to resolve problems identified in the current month's status report.

Appendix A-- Hours by Task Order and Individual Name (see sample): The contractor shall report hours worked by task order and by individual names, including company name.

Electronic Submissions: The contractor may be required to report cost information contained in the monthly status report in electronic format (i.e., CSV file format), in a format to be provided by USPTO.

Attachment 2

SAMPLE
FN01 Monthly Status Report
Task Order Cost Data
REPORT PERIOD: October 2003

TASK ORDER: 03-01

	CURRENT			CUMULATIVE			@ Completion
Rate	BUDGET	ACTUAL	VARIANCE	BUDGET	ACTUAL	VARIANCE	Budget
LABOR HOURS:							
Labor Category							
Tech. Proj. Manager	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Sr. Records Manag Spec.	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Sr. Records Manag Spec.	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Jr Records Manag Spec.	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Jr. Records Manag Spec.	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Technical Write/Editor	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Technical Write/Editor	0.00	0.00	0.00	0.00	0.00	0.00	0.00
SUBTOTAL EMPLOYEE HOURS	0.00	0.00	0.00	0.00	0.00	0.00	0.00
SUBCONTRACTOR HOURS							
Sr. Records Manag Spec.	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Sr. Records Manag Spec.	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Sr. Records Manag Spec.	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Jr Records Manag Spec.	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Jr Records Manag Spec.	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Technical Writer/Editor	0.00	0.00	0.00	0.00	0.00	0.00	0.00
SUBTOTAL SUBS/CONS HOURS	0.00	0.00	0.00	0.00	0.00	0.00	0.00
TOTAL ALL HOURS	0.00	0.00	0.00	0.00	0.00	0.00	0.00
TOTAL LABOR COST	0.00	0.00	0.00	0.00	0.00	0.00	0.00
TOTAL TASK ORDER	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Variance (%)			0.00%			0.00%	
					Percent Budget Used to Date:		0.00%

Attachment 3

UNITED STATES
PATENT AND
TRADEMARK OFFICE

CHIEF INFORMATION OFFICE
UNITED STATES PATENT AND TRADEMARK OFFICE
WASHINGTON, DC 20231
WWW.USPTO.GOV

Office of the Chief Information Officer
Technical Note: IT-212.2-05 TN01
Effective: May 4, 2001
Issuing Office: Office of Data Management

Standard Generalized Markup Language (SGML) and eXtensible Markup Language (XML) Resource Management Guidelines

1. PURPOSE

This technical note establishes procedures for managing Standard Generalized Markup Language (SGML) and eXtensible Markup Language (XML) document resources within the U.S. Patent & Trademark Office (USPTO). The XML Resource Repository stores all versions of DTDs, Schemas, Style Sheets, samples of Document Instances, Public Entities, definitions of USPTO-established XML Namespaces, Templates, and associated documentation. Note: Throughout this document, reference to XML should be construed as including SGML as well.

2. SCOPE AND APPLICABILITY

This technical note applies to all USPTO employees, contractors, and consultants under the direction of the Chief Information Officer. All personnel shall adhere to its contents and the procedures specified herein.

The purpose of this technical note is to avoid unnecessary and costly conflicts in practice among various projects implementing XML and to gain the full benefit of investment in XML technology. The introduction of XML in an organization appears to provide the opportunity for tying automated systems to business rules much more intimately than would be the case without XML. The goal of all interventions in AIS projects described below is to ensure that the interests of all those who have a stake in a system are taken into account when establishing, updating, using, changing, or retiring XML resources.

3. ROLES AND RESPONSIBILITIES

The roles and responsibilities of the XML Registrar, the XML Technology Working Group (TWG) and the AIS System Development Manager are outlined below.

A. XML Registrar (Office of Data Management/Data Administration Division)

As the XML Registrar, the Office of Data Management/Data Administration Division (ODM/DAD) is responsible for controlling access to all approved XML resources. The XML Registrar will conduct internal reviews against logical data models to ensure consistency between logical data elements and the elements used in approved XML resources. The XML Registrar will work with the XML-TWG in comparing new or revised resources against those already approved to ensure maximum re-use of existing XML resources where possible and to assess the impact of any new resources proposed. Upon promotion to the Deployment stage in XML Resource Repository by the SDM with the concurrence of the XML-TWG, resources will be registered as official USPTO named entities and stored in the USPTO Enterprise Information Repository. The Registrar will ensure that XML resources are available to project personnel within the USPTO.

B. XML Technology Working Group

The primary purpose of the XML-TWG is to protect and leverage previous investments in XML resources while supporting the success of new XML projects. The XML Technology Working Group (XML-TWG) will review development of new XML resources, especially XML Schema and DTDs, to ensure conformance with agreed styles and practices; and coordinate changes to resources to maintain consistency across the enterprise and minimize impact on resource users, both internal and external to the organization. Review of XML Schema and DTDs will be a standard LCM step for AIS development projects that include XML resources.

C. AIS System Development Manager (SDM)

The System Development Manager will work with the XML Registrar and the XML-TWG to make use of information already contained in the XML Resource Repository as well as in the USPTO Enterprise Data Model and the USPTO's Standard Data Elements. The System Development Manager will coordinate with the program sponsor regarding XML resources, such as DTDs, schemas, and style sheets.

4. XML Resource Repository Components

The XML Resource Repository identifies the Life Cycle Management (LCM) phases and in addition, users may identify additional stages within the tool. Approved resources are those that have reached the Deployment stage and are ready to enter or have entered the Production stage. Existing projects are encouraged to use the XML Resource Repository for AIS production.

The XML Resource Repository stores all versions of DTDs, Schemas, Style Sheets, samples of Document Instances, Public Entities, definitions of USPTO-established XML Namespaces, Templates, and associated documentation. The approved resources contained in the XML Resource Repository are made available to all project personnel within the PTO via the USPTO Enterprise Information Repository, which is currently available on USPTO workstation desktops and is accessible via the ODM website on the USPTO's Intranet. As part of the configuration management process as defined by the LCM, the AIS development team will provide copies of XML resources, along with other appropriate materials, to the Office of System Product Assurance (OSPA) for loading into the Configuration Management tool.

5. XML Resources Management Procedures

The procedures described here are subject to revision in the light of experiences gained during the months following publication of this Technical Note.

A. XML Resource Repository Procedures

The following outlines the standard procedures for the XML Registrar, the XML-TWG, and the AIS developers to create and manage XML resources.

(1) Any project developing a system that processes content (patent applications, patent file wrappers, trademark applications, granted patents, published trademark registration certificates, the Manual of Patent Examining Procedure, the Trademark Manual of Examining Procedure, or other similar USPTO-owned documents which record or regulate the official business of the USPTO), and uses XML to do so, will use the XML-TWG and the USPTO's XML Resource Repository as the starting place for XML development. The SDM notifies the XML Registrar or XML-TWG of the new project either at a regular XML-TWG meeting, or by email announcing the project. The XML Registrar or XML-TWG will respond by citing related or similar projects and their associated resources.

(2) SDM requests training in XML Resource Repository from XML Registrar for project personnel.

(3) During the Concept phase of the project life cycle, the SDM establishes categories (the structure used to store resources in XML Resource Repository) based on the development phases of the project.

(4) The SDM determines if the XML resources in XML Resource Repository can be used to fulfill the target system's needs. If not, the SDM contacts the XML-TWG for assistance in modifying existing XML resources or developing new ones. Sharing resources can significantly reduce the cost of developing code to process those resources and improve consistency and reliability of products in the eyes of USPTO customers.

(5) Where existing resources require modification as a consequence of the new project, or new resources have significant consequences for existing projects, the interested parties will evaluate the impacts and negotiate the modifications at one or more XML-TWG meetings.

(6) After completing modifications to existing or developing new XML resources, with the concurrence of the XML-TWG, the SDM advances the resources to the Deployment stage in XML Resource Repository .

(7) The XML resources should be tested during the project's development phase.

(8) When XML resources reach the Production stage in XML Resource Repository , the XML Registrar makes them available for public comments through the USPTO Web site. The selected XML resources will also be available in the Enterprise Information Repository.

(9) Any changes to shared XML resources must be coordinated through the XML-TWG. The goal is to reduce or eliminate unexpected consequences for all users of the resources and to ensure that adequate notice is given so that all systems can be updated to reflect the changes.

(10) XML DTDs, schemas, and other XML resources should be incorporated into a project's Detailed Design Document. For further guidelines, please refer to *the Detailed Design Document Technical Standard Guideline IT-212.4-12.* XML resources shall be added to the Configuration Management tool using the procedures outlined in the *Configuration Management Technical Standard Guideline IT-212.2-06.* It is the SDM's responsibility to incorporate XML resources into an AIS's LCM documentation.

These instructions will be refined as the USPTO gains experience with XML Resource Repository .

B. REQUIREMENTS

1. XML Element Naming Convention

Unabbreviated business terminology should be used as the first choice for naming XML resources. Where applicable, the standard data element name should be used. The *Data Element Standardization - Technical Standard Guideline IT-212.2-13* should be used as a reference. Names should be readily understood by users outside the USPTO and by users inside the USPTO who are not familiar with the AIS under development.

Since SGML is not a case-sensitive markup language and XML is, following industry-wide practice, element names should be all lower case. The total length for an element name should not exceed 64 characters, a convention established by the ODM.

Where a name is composed of multiple words, separate the words with dashes or capitalize the initial letter of interior words. For example, `<title-of-invention>` or `<titleOfInvention>`.

2. XML Resource Naming Convention

a) File Naming Convention

The following guidelines provide the naming conventions for the XML resources created within the USPTO. These conventions should be applied to resources developed in SGML, XML, HTML, or any other SGML-based markup language.

-Begin with the title of the document

-Inclusion of a version number in the file name of production files is deprecated. As a rule, version is determined by directory path, as shown in the examples below.

All file names must be followed by a file-name extension that specifies file type. Some examples of typical XML resources have the following customary extensions:

DTD	Document Type Definition
XSD	XML Schema Definition
SGM	SGML document instance
XML	XML document instance
CSS	Cascading Style Sheet
XSL	eXtensible Style Sheet
XSLT	XSL Transformation
DOC	MS Word document
ENT	SGML/XML Entity Definition
TXT	ASCII text document

There should be no spaces in the file name. Words may be separated by hyphens; please do not use underscores.

-Hypothetical examples of filenames, as they will appear in a publicly accessible FTP site, are:
xml.uspto.gov/mathml/v12a/mathml.dtd
xml.uspto.gov/calstabl/v3/calstabl.dtd
xml.uspto.gov/entities/1986/iso-lat1.ent
xml.uspto.gov/entities/1991/isotech.ent
xml.uspto.gov/rb-grant/test/st32-us-grant-019.dtd
xml.uspto.gov/rb-grant/v2.3/st32-us-grant.dtd
xml.uspto.gov/rb-grant/docs/GrantRedBook.doc
xml.uspto.gov/rb-grant/docs/GrantRedBook-header.txt
xml.uspto.gov/rb-application/v1.9/pap.dtd
xml.uspto.gov/efs/specification/current/u-specif.dtd
xml.uspto.gov/efs/specification/current/u-specif.xsl
xml.uspto.gov/efs/specification/v0.8/u-specif.dtd
xml.uspto.gov/team/efw/test/d-efw.dtd

b) XML Resource Header Conventions

For each XML resource, specific header information should be included that details the contents, purpose, and version of the XML resource file. Each XML resource file should contain information pertaining to who owns the XML resource and from which development organization the XML resource stems. The following guidelines should be used when creating an XML resource header. In an SGML or XML resource, the header will ordinarily be a comment associated with the root element (in the case of DTDs or schema) or the first comment appearing in the file. If the file type does not support internal comments, then the header should be in a separate flat ASCII text file with the same name as the resource with the "-header" appended and the file extension *.txt.

Title	Express the title in words that can be easily understood outside the context of the AIS for which the resource

	was developed. Avoid acronyms and abbreviations.
Version Number (Version numbers in file names are deprecated.)	Add the current version of the file in the format, "vx.xx" where the x's are replaced by a numerical sequence incremented whenever the file is updated, starting with "0.01" Versions produced before production starts should be numbered "v0.xx." Subsequent to the start of production, revised versions should be numbered "v1.xx" and higher. Each change to the version number must be recorded in the resource's Revision History.
Note	A brief explanation of the background and purpose of the resource.
Development Organization Information	Name and address of the organization developing the resource. This will always be U.S. Patent & Trademark Office.
Responsible Party	Give the primary organization name that owns the resources.
Revision History	The first entry in the Revision History should always be: "Original Version 0.1 - [date]; [responsible party]". Add a new entry in the revision history whenever there are changes made, including the date. Within the entry, provide details of each change made. Within each entry, note any increment of the version number.

An example of a DTD header is below.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- DOCTYPE patent-application-publication [ -->

<!-- DOCUMENT TYPE DEFINITION FOR UNITED STATES PATENT APPLICATION PUBLICATIONS
Reference this DTD as PUBLIC "-//USPTO//DTD PAP V1.3 2000-09-06//EN"
Alias: Application Red Book (ARB)

Development Organization Information: the U.S. Patent & Trademark Office

Note:

The structure is for a patent application electronic document (Pre-grant U. S. publication).
It contains all elements, content, and references to external entities that constitute the
patent application, including bibliographic, abstract, description, sequence listing, claim,
and drawing information.


Responsible Party:

Information Products Division
U.S. Patent and Trademark Office
Crystal Park 3, Suite 441
Washington, DC 20231
-->

<!-- ***** START REVISION HISTORY *****

Pending Issues/Comments:
1) The CALS Exchange table mode does not support spanning (spanspec) columns.
..Since the table related elements have been removed and replaced with a
..reference to the CALS Exchange XML dtd, this may conflict with ESF
..input. Need to investigate how to implement spanspec within PAP for
..EFS compliance.
```

```
2)  The PAP sample data includes a hard coded reference to the DTD using
..a full path. Need to explore using a URI/URL.

Revised 2000-09-06
1)  Changed version to V1.3 and build date to 2000-09-06.
2)  Changed element usc371-date to optional since it will not be included
..on the published application cover page.
3)  Added optional element military-address to the address element.
..The data capture contractor will extract the military address text
..from the address line text.
4)  Modified the residence element to distinguish between US and
..non-US residences.

Revised 2000-08-22
1) Removed addition-to related application code.
2) Changed version to V1.2 and date to 2000-08-22.

Revised 2000-08-08
1) Changed the xml encoding from "ISO-8859-1" to "UTF-8"

Revised 2000-08-02
1)  Moved the botanic model from the specification (in front of
..the background-of-invention) to the bibliographic (after the
..title-of-invention) section.
2)  Within the patent application DTD, the sequence-cwu model was modified
..to include an object reference for patents with sequence listings that
..are not to be published. The sequence-cwu model changed:
..From: (number,(sequence-list-old-rules | sequence-list-new-rules | table),image*)
..To: (number,(sequence-list-old-rules | sequence-list-new-rules | table | object-
reference),image*)
3) Moved element sequence-cwu to before subdoc-claims.
4) Added a-371-of-international to the patent application DTD (missing)
5) Added reissue-of to the patent application DTD (missing)
5)  Renamed element "substitute-for" to "substitution-for" so it would
..match the EFS counterpart element.
6)  Added footnote to the paragraph content model.
..Moved out of the external references.
8) Changed version to V1.1 and date to 2000-08-02.

. . .

Revised 2000-04-04
..Changed version to 0.2 and date to 2000-04-04.
..Added a new element, number, to the content model of paragraph, biological-deposit
...program-listing-deposit, and sequence-cwu. Used for object sequence number.
...See specification for markup instructions.
..Added a new attribute, inid-code, to almost all the elements in
...subdoc-bibliographic-information. This attribute will contain the INID code as
...assigned by data-capture contractor and which appears on the page-composed
...image next to that element. See specification for details.

Revised 2000-03-27
..Extensive revisions based on PGPub DTD Team meetings over the past two months.
..First official distribution of the DTD on this date.

Created 2000-02-16
********** END REVISION HISTORY ********** -->
```

3. Data Modeling Activities

Mapping Matrix

A mapping matrix between elements in a DTD or schema to either the logical data model or to object data in an object-oriented design might be required. Depending on the AIS development approach, these mappings may be produced using traditional mapping documentation (spreadsheets) or via Unified Modeling Language (UML). This matrix will map the transformation from the attributes of the logical data model to the elements of the XML DTD or schema (see example in Figure 2 below). For assistance in preparing the mapping matrix, please contact the Data Administration Division staff.

For AIS's using object-oriented design and UML, please contact the Data Administration Division for assistance on how to map these data elements. Guidelines for developing a logical data model can be found in the *Detailed Design Document (DDD)-Technical Standard Guideline* and *Data Element Standardization-Technical Standard Guideline.*

An example of a logical data model is shown in the below figure.

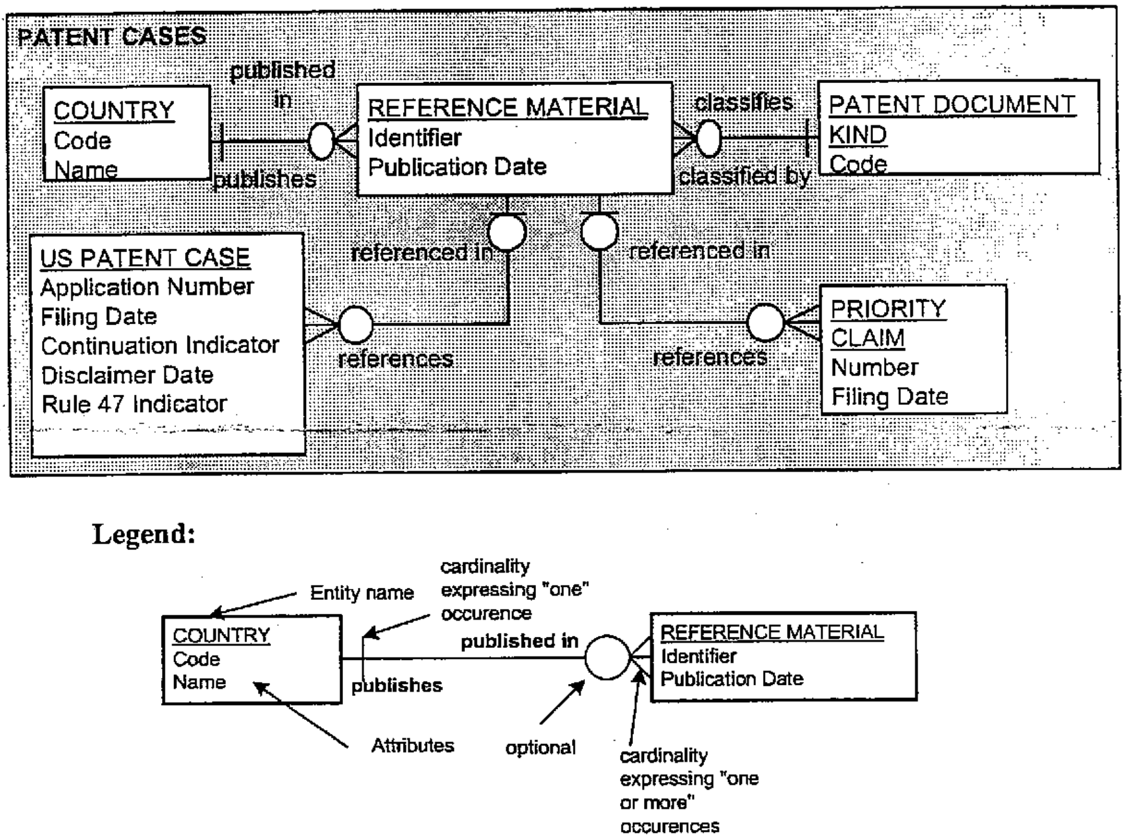

Figure 1—Example of a Logical Data Model

LOGICAL DATA MODEL			DTD/SCHEMA	SCHEMA only	
Attribute Name	*Length*	*Optionality*	*Element Name*	*Length*	*Optionality*
			document-identification		
REFERENCE MATERIAL Identifier	12	Mandatory	doc-number		Mandatory

PATENT DOCUMENT KIND Code	1	Mandatory	kind-code		Mandatory
REFERENCE MATERIAL Publication Date	8	Mandatory	document-date		Mandatory
COUNTRY Code	3	Mandatory	country-code		Mandatory
			domestic-filing-data		
US PATENT CASE Application Number	8	Mandatory	application-number		Mandatory
US PATENT CASE Filing Date	8	Optional	filing-date		Optional
US PATENT CASE Rule 47 Indicator	1	Mandatory	rule-47-flag		Mandatory
US PATENT CASE Continuation Indicator	1	Mandatory	continued-prosecution-application-flag		Mandatory
			foreign-priority-data		
PRIORITY CLAIM Number	10	Mandatory	priority-application-number		Mandatory
PRIORITY CLAIM Filing Date	8	Mandatory	filing-date		Mandatory

Figure 2—Example of A Mapping Matrix

4. Reusable XML Resource Components

The approved XML resources in XML Resource Repository should be reused as much as possible. The SDM is required to implement existing XML resources in XML Resource Repository if they are suitable, or can be modified to be suitable, before developing new ones. Doing so can reduce development time for the resources as well as for software to process the resources.

Appendix A
Guideline for Developing the XML Resources

This appendix provides the recommended guidelines for system developers to create XML resources.

A. Existing Document Analysis

A thorough analysis of the representative documents and the project requirements is recommended. The business representative(s) should provide the development team with all relevant specifications and reasonable access to an adequate set of documents concerning the type of document for which the XML resource is to be developed. The purpose and outcome of the documentation analysis is to identify structure, format, and content of the given document and to prepare for the development of the XML resources.

The outcome of document analysis should result in the following:

- determine the stakeholders to include users, management, and customers
- identify the scope of the analysis and project (applicability within the organization)
- define a DTD strategy (simple vs. complex, modular vs. in-line, DTD vs. XML Schema)
- identify the root structure of the document class
- identify the logical structures in the document class
- identify the hierarchy of the elements/document tree
- identify specific styling requirements as distinguished from informal styling conventions

B. XML Resource Development

Prior to writing the DTD, it is important to determine the setup of the DTD. It is important to consider:

- If the new XML resource should consist of multiple components; and
- The reusability aspects of each piece of the components if they are to be called or referenced by other resources

It may be useful to decompose the XML resource into components which are stored as external entities. A component is a discrete portion of a DTD or schema that can be reused or called by other XML resources. These may be as small as a single element within that DTD or Schema, or it may be a set of elements combined that create a single logical section of a document type. Such components are often common to more than one document type. For example, the "table" component of a document type contains all the elements necessary to represent the complete structure of a table. The DTD specifying markup for tables (common to any document type that uses tables) is usually in a separate file and called in or accessed through a parameter entity. There are similar DTDs for mathematics markup and for chemistry markup. A DTD which incorporates external entities of this kind is expanded by the parser in a production system to include the declarations contained in the external DTDs. Most DTDs will contain references to external entities which are commonly used within the USPTO. A parameter entity is a pointer to information contained either within the current DTD file or in an external file. Parameter entities may be used to incorporate the content of additional DTDs, components of DTDs, or other files into a DTD. Common components that are maintained as separate, secondary files for the DTD are:

- DTD default structures;
- Special fonts (character entity files);
- Table structures;
- List structures;
- Reference structures;
- Graphic notations; and
- Configuration parameters.

When developing the DTD, case sensitivity must be kept in mind. While SGML is not a case-sensitive markup language, XML is. As such, where possible, element names should be all lower case. Names should be kept to 64 characters or less, with multi-word names underscored (`<first_named_inventor>`), hyphenated (`<first-named-inventor>`), or use "camel" capitalization (`<firstNamedInventor>`). Hyphenation is preferred as it is the easiest to type.

The XML resources should be validated by at least two parsers. Parsing an XML resource does not determine if it is accurate for the documents for which it is intended but, rather to verify if the source code of the resources is syntactically correct. For the parser products, please refer to the Technical Reference Model.

	used to link the content of additional DTDs, components of DTDs, or other files into a DTD.
Public Entities	Public Entities are external to the document instance, schema, or DTD. A public entity is defined using external naming conventions that identify the standard used for the external file, the type of file being referenced (external DTD fragment, character set, etc.), and a unique location or name where that file can be located. With XML, the unique location is often a URL, though in many cases, depending on the longevity required for the identifier, the unique location may be more open. In such cases, a SYSTEM identifier must be mapped to the public identifier.
SDE	Standard Data Element
SDM	System Development Manager (*see Section 3.C*)
Schema	An XML Schema is an XML language for describing and constraining the content of XML document.
SGML	Standard Generalized Markup Language; the "parent" of both XML and HTML; a syntax for structurally and hierarchically representing content independent of its format.
XML Registrar	An ODM staff member responsible for administering and managing all USPTO XML resources.
Style Sheet	A specification of the rendering of a document type or a document instance.
Tag	Tags are text structures that mark the beginning and end of elements within SGML or XML documents. Tags are either paired (start tag and end tag) or empty (only one tag which serves both purposes).
Template	A gauge in creating the XML resource to ensure that data remains accurate, reliable, and consistent.
UML	Unified Modeling Language
URL	Universal Resource Locator
USPTO	United States Patent and Trademark Office
XML	eXtensible Markup Language; the middle "sibling" between SGML and HTML; XML is a profile of SGML, restricting many of the optional aspects of SGML to a single choice, but is more robust and flexible than HTML. XML maintains the delineation between content and format, but removes much of the complexity of SGML.
XML Namespaces	XML Namespaces are used to distinguish specific element names when elements are mixed and matched from different XML applications.
W3C	The World Wide Web Consortium was created in October 1994 to lead the World Wide Web to its full potential by developing common protocols that promote its evolution and ensure its interoperability. W3C has more than 400 Member organizations from around the world and has earned

international recognition for its contributions to the growth of the Web.

[SIGNED]
Holly Higgins
Director, Office of Data Management

May 4, 2001
Date

Instructions for FN07, Resource Estimate:

Deliverable Number: FN07

Title/Description: Resource Estimate

Frequency of Submission: As Required

No. of Copies: 5

Submission is Due: 5 working days after receipt of Government Technical or Contracts Direction. Subsequent Submissions due as required.

Government Assistance Required: Yes

Government Response Due: 10 working days after receipt of resource estimate. The government will either authorize or reject the estimate in writing.

Remarks: Once the Resource Estimate has been approved, the Contractor will provide updates to the TM02, Task Management Plan.

Format/Content Requirements and Instructions: Resource Estimates are provided to the Government to estimate additional work in an existing Task Order, to estimate new or unauthorized tasks, or to document the descoping of a Task Order. The Resource Estimate consists of the following sections:

Technical Approach
Schedule
Deliverables
Sizing Assumptions
Resource Estimate Summary

Technical Approach: The technical approach is a narrative section that states the overall task objectives and the basic activities necessary to achieve the objectives.

Schedule: The schedule is a bulletized list of the major milestones and deliverables to be performed in the task. Each item will include a scheduled completion date.

Deliverables: The major contract deliverables are listed with a title and CDRL number or a highly descriptive title if no CDRL is assigned.

Sizing Assumptions: The sizing assumptions address the basis for the resource estimate. The source of the requirement will be referenced (for example, a task objective statement or a Government request for an estimate). There will be an explanation of the assumptions used in estimating the various direct cost elements (for example, labor, travel) and a list of other direct costs and materials items required for successful completion of the task.

Resource Estimate Summary: A resource estimate summary provided to the Government (see sample sheets 1 and 2) with the total cost per contractor cost element of the described task or activity. If there are multiple Task Orders or CLINs involved in the estimate then the resource estimate will separate the estimate and provide a cost column for each Task Order and/or CLIN along with a total column for the total cost of the task.

Attachment 5

FN07 RESOURCE ESTIMATE SUMMARY
SAMPLE– SHEET 1

Ref Code	Labor Category	Site	Company	GFY-03		GFY-04		GRAND TOTALS Hours/Qty	GRAND TOTALS Amounts
03-xx Task Order A								Totals: 02-xx Task Order A	
	Tech. Proj. Manager	Crystal City	XYZ	10.0	800	10.0	800	20.0	1,600
	Senior Records Management Spec.	Crystal City	XYZ	10.0	800	10.0	800	20.0	1,600
	Junior Records Management Spec.	Crystal City	XYZ	-	-	8.0	640	8.0	640
				20.0	$ 1,600	28.0	$ 2,240	48.0	$ 3,840
									-
TOTAL DIRECT LABOR					$ 1,600		$ 2,240		$ 3,840
SUBCONTRACTORS:								-	-
	Senior Records Management Spec. Sι	Crystal City	ABC	10.0	$ 800	10.0	$ 800	20.0	1,600
	Technical Writer/Editor	Crystal City	ABC	10.0	$ 800	10.0	$ 800	20.0	1,600
TOTAL SUBCONTRACTOR LABOR				20.0	$ 1,600	20.0	$ 1,600	40.0	$ 3,200
		Total Hours		40.0		48.0		88.0	
TOTAL PROPOSED COST 03-xx Task Order A					$ 3,200		$ 3,840		$ 7,040

NOTE: Hour and Cost numbers shown are imaginary and for illustrative purposes only.

Attachment 6

FN07 RESOURCE ESTIMATE SUMMARY
SAMPLE--SHEET 2

Ref Code	Labor Category	Site	Company	Current TM02 Totals		New FN07 Totals		Revised Budget if Appvd.	
				Hours/Qty	Amounts	Hours/Qty	Amounts	Hours/Qty	Amounts
03-xx Task Order A								Totals: 03-xx Task Order A	
	Tech. Proj. Mgr.	Crystal City	XYZ	50.0	4,000	20.0	1,600	70.0	5,600
	Senior Data Quality Management Spec.	Crystal City	XYZ	40.0	3,200	20.0	1,600	60.0	4,800
	Junior Data Quality Management Spec.	Crystal City	XYZ	20.0	1,600	8.0	640	28.0	2,240
TOTAL DIRECT LABOR				110.0	$ 8,800	48.0	$ 3,840	158.0	$ 12,640
SUBCONTRACTORS:									
	Senior Data Quality Management Spec.	Crystal City	ABC	20.0	$ 1,600	20.0	$ 1,600	40.0	3,200
	Technical Writer/Editor	Crystal City	ABC	30.0	$ 2,400	20.0	$ 1,600	50.0	4,000
TOTAL SUBCONTRACTOR LABOF				50.0	$ 4,000	40.0	$ 3,200	90.0	7,200
TOTAL PROPOSED COST 03-XX TASK ORDER A				160.0	$ 12,800	88.0	$ 7,040	248.0	$ 19,840

NOTE: Hour and Cost numbers shown are imaginary and for illustrative purposes only.

Attachment 7

Data Quality Management
at the
United States Patent and Trademark Office

(A brief "how-to" instruction for specifying and executing a Total Data Quality Analysis project)

prepared by:
Office of the Chief Information Officer
Office of Data Management
Data Administration Division

Revised March 1998

Introduction

During the current period of rapid PTO information systems development, the functions and processes in many legacy automated information systems are being merged and consolidated. Stand alone legacy information systems that do not communicate to share data are being redesigned to form an interoperable and shared data environment. While focusing on achieving this open systems environment, data quality issues are being identified as important factors inhibiting system integration, data migration and conversion, and information system interoperability.

Different business uses of data impose different data quality requirements. Only actual users of a data set can determine the fitness for use of the data. Data that is of sufficient accuracy and timeliness for use by one PTO business unit, may not have an acceptable level of quality for use by another business unit or customer. Costs of inaccurate or inadequate data can be steep. Problems with data quality can result in tangible and intangible damage ranging from increased system development time, additional maintenance costs and loss of customer/user confidence, to missed business opportunities for growth.

Current research indicates that accuracy of data instances within data sets is only one aspect of data quality and is often not the most important aspect. While accuracy may be the easiest to quantify and measure, other aspects must be addressed during the data quality analysis of any data set. Data quality analysis must address the concepts of accessibility, interpretability, relevancy, and accuracy of the data sets being examined. This analysis is performed for each defined user group of the data set.

Managing data quality at the PTO is essential to mission success. Business managers require quality data delivered in a useable format at the right time. This document describes policy and procedures to assure that data is meeting the quality characteristics required for use by all business units in the PTO. In addition, implementing these guidelines for improving data quality will lower the costs of automated support to the PTO functional community and streamline the exchange of technical and management information.

PTO Data Quality Management

Table 1 summarizes the six categories of PTO data quality characteristics and conformance measurements. The CIO is developing methods to describe ways to improve data quality, to assure that: (1) users (customers) of data are involved in improving data quality, (2) predetermined requirements for excellence are defined in terms of measurable data characteristics, and (3) data conforms to these requirements.

Data Quality Characteristic	Definition	Example Metric
Accuracy	A qualitative assessment of freedom from error, with a high assessment corresponding to a small error. (ISO in FIPS Pub 11-3).	Percentage of values that are correct when compared to the actual value. For example, M=Male when the subject is Male.
Completeness	The degree to which values are present in the attributes that require them. (*Data Quality Foundation*)	Percentage of data fields having values entered into them when a value is expected.
Consistency	A measure of the degree to which a set of data satisfies a set of constraints. (*Data Quality Management and Technology*)	Percentage of matching values across tables/files/records.
Timeliness	A synonym for currency representing the degree to which specified data values are up to date. (*Data Quality Management and Technology*)	Percentage of data available within a specified threshold time frame (e.g., days, hours, minutes).
Uniqueness	The state of being the only one of its kind; sole. Being without an equal or equivalent; unparalleled. (*The American Heritage Dictionary*)	Percentage of records having a unique primary key.

Validity	The quality of data that is founded on an adequate system of classification (e.g., data model), which is rigorous enough to compel acceptance. (*DOD 8320.1-M*).	Percentage of data having values that fall within their respective domain of allowable values.

Table 1: Core Set of Data Quality Requirements

Figure 1 illustrates the PTO Data Quality Management process. Establishing the Data Quality Management environment builds up management and infrastructure support. Then, appropriate data quality projects are identified and levels of required data quality are defined. Implementing selected data quality projects is performed in four steps detailed later in this document. The Data Quality Management process includes evaluating the data quality management process by reviewing data quality goals and benefits, and improves overall methods used to manage data quality.

1. Establish PTO Data Quality Management Environment

Securing a commitment to the Data Quality Management process is accomplished by establishing the data quality management environment between information system project managers and establishing conditions to encourage team work between functional and information system development professionals. The CIO is committed to Data Quality Management at the PTO and supports all data quality initiatives, especially in conjunction with migrating and converting legacy data to new hardware platforms during re-engineering development projects.

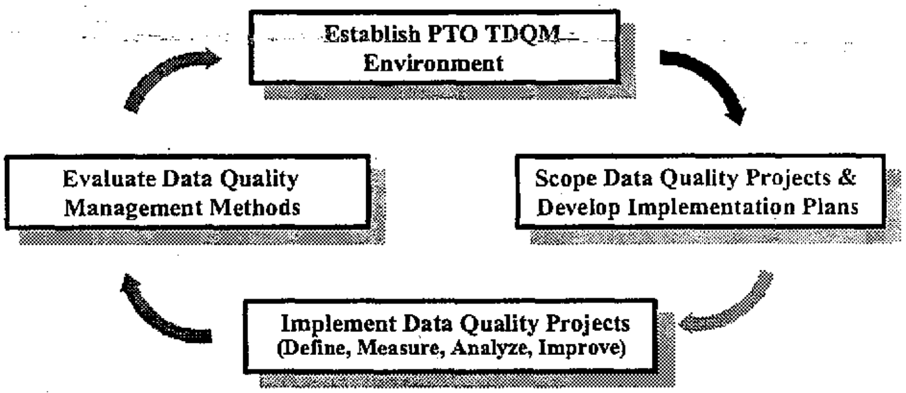
Establish PTO TDQM Environment
Scope Data Quality Projects & Develop Implementation Plans
Implement Data Quality Projects (Define, Measure, Analyze, Improve)
Evaluate Data Quality Management Methods

Figure 1: Data Quality Management Process

The CIO selects information system development efforts to participate in pilot projects to demonstrate the benefit of data quality analysis during system design/development and legacy data migration. The CIO Data Administration Division in the Office of Data Management coordinates data quality analysis projects with system developers and functional users of the target migration information system. Functional users of legacy information systems know data quality problems of the current systems but do not know how to systematically improve existing data. Information system developers know how to identify data quality problems but do not know how to change the functional requirements that drive the systemic improvement of data. Given the existing barriers to communication, establishing the data quality environment involves participation of both functional users and information system administrators.

Projects selected for immediate support by the CIO will meet the following criteria.

- Conditions exist that indicate a high chance of success for the data quality analysis (current project management, developer, and functional user community support for the analysis).
- Poor quality data in the target system have potential high failure costs to the PTO.

- Significant improvements can be made in a short amount of time (data quality problems are already apparent to the user community).

2. Scope Data Quality Projects & Develop Implementation Plans

For each data quality analysis project selected, the data quality project manager defines the scope of the project and defines the level of analysis that will be the most beneficial for the project under question. Draft an initial plan that addresses the following elements.

- Task Summary: Project goals, scope, and potential benefits
- Task Description: Describe data quality analysis tasks
- Project Approach: Summarize tasks and tools used to provide a baseline of existing data quality
- Schedule: Identify task start, completion dates, and project milestones
- Resources: Identify resources required to complete the data quality assessment. Include costs connected with tools acquisition, labor hours (by labor category), training, travel, and other direct and indirect costs
- Deliverables: List reports and/or products to document the result of the data quality project. At a minimum, deliverables should include:
    a. Data Quality Baseline Assessment—Document current data quality problems. Include exception reports on data that does not conform to established standards or business rules.
    b. After Action Report—Technical report on the data quality improvements implemented. Include description of actions taken to improve data quality, rationale for taking the actions, lessons learned, and improvement metrics.

3. Implement Data Quality Projects (Define, Measure, Analyze, Improve)

A data quality analysis project consists of four activities. The data quality project manager performs these activities with input from the functional users of the data, system developers, and data base administrators of the legacy and target data base systems.

- Define: Identify functional user data quality requirements and establish data quality metrics
- Measure: Measure conformance to current business rules and develop exception reports
- Analyze: Verify, validate, and assess poor data quality causes. Define improvement opportunities
- Improve: Select/prioritize data quality improvement opportunities

Improving data quality may lead to changing data entry procedures, updating data validation rules, and/or use of PTO data standards to prescribe a uniform representation of data used throughout the PTO.

4. Evaluate Data Quality Management Methods

The last step in the PTO Data Quality Management process is to evaluate and assess progress made in implementing data quality initiatives and/or projects. All participants in the Data Quality Management process (functional users, program managers, developers, and the Office of Data Management) should review progress with respect to: (1) modifying or rejuvenating existing methods to data quality management and/or (2) determining whether data quality projects have helped to achieve demonstrable goals and benefits. Evaluating and assessing data quality work reinforces the idea that Data Quality Management is not a program, but a new way of doing business

Executing PTO Data Quality Management Methodology (Define, Measure, Analyze, Improve)

The overall objectives of the PTO Data Quality Management approach are to assess and validate data quality problems, identify root causes for data quality problems, and improve the quality, utility, accessibility, and shareability of data at the PTO.

Define Current Data Quality

Defining the data quality for an information system based on how the data is used is not a trivial task. Good data quality analysis requires clearly understanding the data by completing the following activities.

- Analyze historical data problems
- Identify and review information system documentation
- Capture business rules and data quality metrics (how the users measure data quality)

Specific data problems are linked to business rules and generic and specific rule sets are established to measure how good the data is within an information system. Table 2 illustrates several rule sets and an acceptable method of documenting known data quality problems.

Historical Data Problem	Rule Type	Generic Rule Set	Specific Rule Set
Equipment identifier fields are often blank.	Null Constraints	If the equipment identifier is blank or null, then, error.	Select equip_id from equip or equip_id =' ' or equip_id = NULL;
The code for DEBIT/CREDIT is sometimes not 'D' or 'C'.	Domain Validation	If Debit/Credit code is not 'D' or 'C', then, error.	Select debit_code from transaction where debit_code not = 'D' or 'C';
The value of unit price is not greater than zero.	Operational Rule Set	If unit price = $00.00, then, error.	Select * from equip where unit_price = 00.00;
The total charge for a credit card purchase exceeds $25,000.	Business Rule Validation	If total_charge is greater than $25K, then, error.	Select total from charge when total > 25000;

Table 2: Examples of Data Quality Rule Set Generation

Establish a set of rule sets and measurements to execute as SQL statements or as data quality filters in an automated data quality assessment tool. The rule sets represent the data quality metrics used to judge conformance of data to PTO business rules. Data quality project managers use PTO data standards as the basis for establishing rule sets. PTO data standards provide valid values for many common data elements such as Country Code, Country Name, and State Abbreviation. The standard data elements provide format, length/precision indicators, and the acceptable range of values that are used as data quality tests/metrics.

At this point in the analysis, the data quality analyst assesses the accessibility, interpretability, and relevancy of the data to the defined users of the data set. While these concepts are not easily quantified, they must be considered in order to obtain a clear picture of the users' needs regarding overall data quality when using this data set.

Measure Data Quality.

Measure data quality in five stages.

- Determine the approach to be used to measure data quality
- Apply the rule sets to the tables/files/records that are to be checked
- Flag suspect data in error reports
- Validate and refine the rule set
- Develop metrics reports to categorize data quality problems

There are two basic approaches used to measure data quality. The first approach is to measure conformance to business rules and PTO data standards by executing the rule sets on the same machine and/or data server that supports the legacy information. The data quality checks are written as SQL scripts to test data conformance. This approach is possible at the PTO only for those legacy systems using relational DBMS structures.

Figure 2 illustrates the second approach to measure conformance to business rules. This approach is used in data migration situations where the legacy data is not stored in relational DBMS structures. The data is moved to an interim environment prior to loading data to the target hardware platform. At the PTO, the legacy data structures are simulated in Oracle data base tables in a "staging area" for the data. The data sets in the staging area are tested using the rule sets or data quality filters developed to assess conformance to established PTO business rules. Exception data, or data that fails to pass the rule set, is researched to determine why the data did not conform to the rules. Researched data sets are corrected and passed again through the filter set to validate the corrections. This approach provides the ability to generate metric reports to illustrate how well (or how poorly) the data conforms to PTO business rules and data quality standards. This approach assures that only accurate, complete, and timely data migrates to the target data environment.

Measure data quality by defining up to four levels of analysis.

- Level 1 analysis tests for the existence of values in a specific table column, and if there is a value, verifies that the value is acceptable (e.g., value in valid domain set, value in range, valid format, etc.). Tests are always based on what is reasonable and pertinent to the project. If a column in a legacy data table is not used by the target information system, it is not tested.

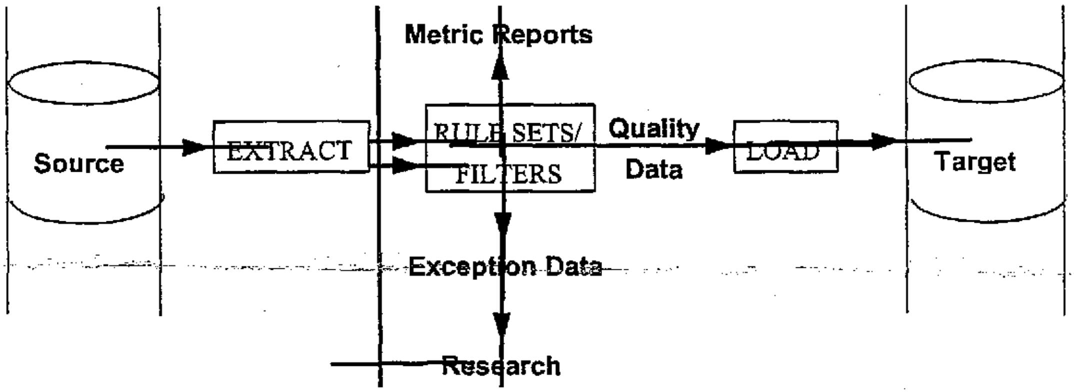

Figure 2: Performing Data Quality in Interim Data Environment

- Level 2 analysis tests referential integrity in the legacy data. Perform this analysis in two directions: parent to child, and child to parent. The two-directional tests identify parent records that have lost required child records, and establish which child records have no parent records. Check cardinality rules at this level. Rules checked might include: a parent record must have at least one child record, or a parent record must have exactly two child records for a specified condition.
- Level 3 analysis documents and tests the relevant business rules for the data set. For example, if a certain GL_Account Code is in the 5000 series, certain other values in the table may or may not be required (i.e., values found where there should be no values are also considered errors).
- Conduct Level 4 analysis to change the legacy data prior to migration to the target platform or if data transformation will occur during the actual migration of the data set. Define transformation rules and specify when they will be applied. For example, develop a mapping table to transform old office symbols to their current equivalent during migration of a data set to the Financial Subject Area of the PTO Data Warehouse.

A thorough knowledge of the data set as it resides on the legacy platform, the current and projected uses of the data set after migration of the data set, and knowledge of the target data base structures are essential before beginning this analysis. Data quality analysis is useful during Functional and Data Requirements Definition and Detailed Business Area Description development in the PTO Life Cycle Management methodology. Preparing system documentation for the data quality baseline assessment enhances knowledge about the current and target data environments and adds value to the system development life cycle.

Analyze Data Quality

Use metric reports to analyze data quality problems. Obtain the assistance of functional and technical data experts most familiar with the data and processes supported by the information system. The analysis phase identifies and validates the following.

- Key data quality problems from the metrics reports and user feedback
- Root causes for data quality problems
- Cost impacts connected to correcting the root causes of data quality problems
- Solutions for improving the processes that are used to create and maintain data to minimize data errors

Metric Reports

Analyzing metrics reports provides an opportunity to identify and validate the types of existing data quality problems. Metrics reports provide an overall view of data quality within an existing data set. Metrics reports also provide a method for measuring improvement shown over time based on implementing data quality process improvements. The Office of Data Management supports the use of graphical reports produced by an automated data quality analysis tool to check data quality. Although SQL scripts and programs can execute data quality rule sets/filters, it is best to use tools specifically designed to perform data quality analyses with capabilities to easily:

- Audit the performance of data quality checks;
- Track historical records of prior data quality checks, and
- Graph data quality trends over time.

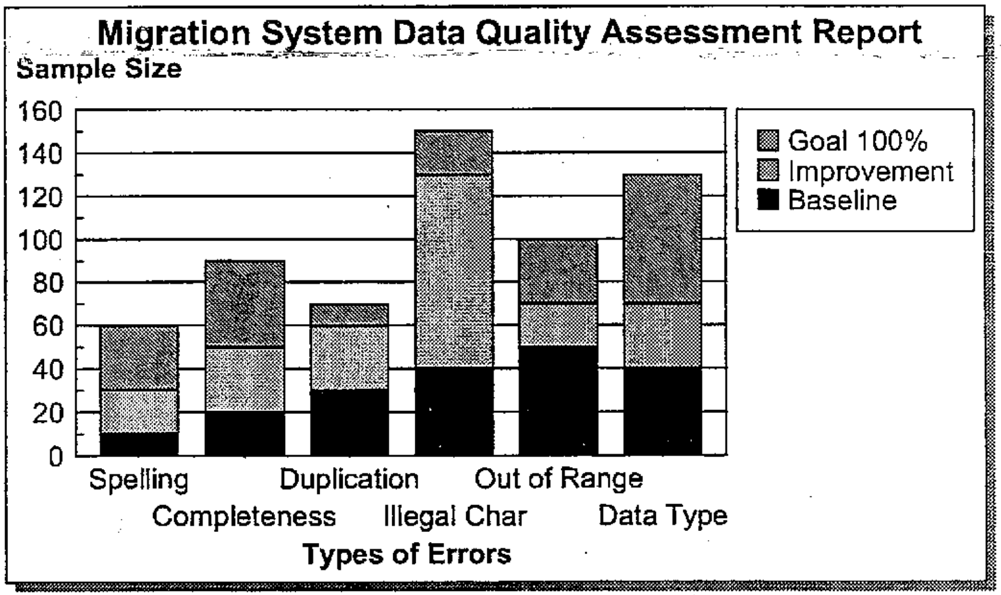

Figure 5: Sample Data Quality Metrics Report

Answer key business questions with metrics reports:

- In what areas did a significant number of errors occur?
- Did certain types of errors occur more frequently than others?
- What is the best area on which to concentrate efforts to obtain the greatest improvement in data quality?

Categorize Data Quality Problems

Analyzing errors that occur infrequently may reveal the cause of a specific error but, is not likely to identify a broad-based systemic problem. Fixing small problems (e.g., a one time data entry error) may offer anecdotal evidence to support the value of data quality assessments. However, benefits are greater when the focus is on systemic root causes of data errors.

Examine possible causes from several points of view such to determine root causes of data quality problems:

- Process Problem: Process problems cause the majority of data errors. For data errors categorized as process problems, examine existing processes that support data entry, assignment and execution of data quality responsibilities, and methods used to exchange data. Use knowledge of these activities in relation to data errors to find and recommend actions to correct deficiencies.
- System Problem: Data problems often stem from system design deficiencies acerbated by poorly documented modifications and incomplete user training and/or user manuals, or systems that are being extended beyond their original intent. An examination of system modifications, user training, user manuals, and engineering change requests and problem reports can reveal information system problems that can aid in improving data quality.
- Policy and Procedure Problem: Analyzing data errors may reveal either conflicting guidance in current policy and procedure, lack of appropriate guidance, or failure to comply with existing policy/procedure. Examine existing directives, instructions, and standard operating procedures to resolve the root cause of data errors.
- Data Design Problem: The data base itself allows data errors to creep into data values as a result of batch loads. the use of incomplete data constraints, and/or the inappropriate specification of user privileges. Examining batch load scripts or programs eliminates possible data errors attributed to circumventing data integrity constraints. It is also advisable to examine the implementation of:

    1. Primary key constraints
    2. Null and not null data specifications
    3. Unique key constraints and indexes
    4. Data base triggers
    5. Stored functions and procedures
    6. Referential integrity specifications (e.g., cascading deletes).

Cost Impacts

One of the real challenges in data quality management is how to assess costs connected to correcting root causes for data quality problems and costs associated with not correcting the problems that damage data. Focus on defining the costs incurred to create and maintain the data and the cost of determining if the data values are acceptable, plus any cost incurred by the organization and the end user because the data did not meet requirements and/or end user expectations.

Direct costs to the PTO include:

- Controllable costs: Recurring costs for analyzing, correcting, and preventing data errors;
- Resultant costs: Internal and external failure costs of business opportunities missed; and
- Equipment and training costs: Costs for data quality tools, ancillary hardware and software, and training required to prevent, appraise, and correct data quality problems.

If possible, compare two or more alternatives for improving data quality. Estimate the controllable, equipment, and training costs for each alternative. Include an estimate of labor hours devoted to prevent, appraise, and correct problems.

Resultant costs and indirect costs are more difficult to quantify. Assess these costs wherever possible to adequately measure the impacts of poor data quality. For example, the inability to match payroll records to the official employment records can cost millions in payroll overpayments to retirees, personnel in leave without pay status, and "ghost" personnel. Inability to correlate purchase orders to invoices may be a major problem in unmatched disbursements. Resultant costs, such as payroll overpayments and unmatched disbursements, may be significant enough to warrant extensive changes in processes, systems, policy and procedure, and information system data designs.

Recommending Solutions

Data quality analysis is not complete until recommendations are provided on the actions to be taken to improve the data quality within an information system. Recommendations may include making the data more easily accessible to different user groups within the PTO or making available better documentation in order to use the data more effectively in decision making. Solutions should not focus solely on creating perfectly accurate data sets. Recommendations should be supported by:

- Identification of the key data quality problems to be solved;
- Specification of the root causes for data quality problems; and
- Analyzing cost impacts connected to taking (or not taking) the corrective actions necessary to improve the data.

If several alternatives are available, determine the level of risk that accompanies each alternative. Risk mitigation should favor small incremental improvements that are quick and easy to implement and have a high return on investment.

Improve Data Quality

After defining the systematic actions that will improve data quality within a data set, perform two additional activities. First, functional proponents for the information system and the system administrators review the recommendations to determine the feasibility of each recommendation. During the review of recommendations, consider how solutions will affect end users, functional processes, system administration, policy, and data design. Additional factors influencing the go ahead on recommendations include: (1) the availability of resources needed to accomplish the improvement, (2) the schedule of software releases, and (3) changes to the information system hardware and/or telecommunications environment. Any one of these factors can influence the execution of data quality improvement recommendations.

The second major activity in improving data quality is to execute the recommendation(s) and monitor the implementation. In parallel with root causes for data quality problems, improvement work tends to fall into four categories.

- Process Improvement: Improve the functional processes used to create, manage, access, and use data. Functional process changes may encourage centralized data entry, eliminate non-value added activities, and place data quality responsibilities where data is entered into the data set (e.g., certification of data)
- System Improvement: Software, hardware, and telecommunication changes can improve data quality. For example, security software can minimize damage done by malicious updates to data bases by unauthorized users. Hardware improvements may make batch loads faster and thereby make it unnecessary to turn off edit and validation constraints when loading data to a data base. Telecommunications improvements (e.g., increasing bandwidth) may provide easier access to data and improve both the accuracy and timeliness of data. Other system improvements may include updating end user, operation, and maintenance manuals, and providing additional user training.
- Policy and Procedure Improvement: Resolve conflicts in existing policies and procedures and institutionalize behaviors that promote good data quality. Develop Standard Operating Procedures for the information system to document the data quality rule sets/filters used to measure data quality. Perform periodic data quality checks as part of the Standard Operating Procedures to increase data quality.
- Data Design Improvement: Improve the overall data design and use PTO data standards. Adding primary key constraints, indexes, unique key constraints, triggers, stored functions and procedures, controlling administration of user privileges, enforcing security features, and referential integrity constraints can improve data base design.

Summary

PTO guidance on data quality management emphasizes improving data quality to ensure that: (1) users of data are involved in improving data quality, (2) predetermined requirements for excellence are defined in terms of measurable data characteristics, and (3) data conforms to these requirements.

The approach to achieve these goals consists of four steps.

- Establish the Data Quality Management environment where key participants include project managers, functional users, system developers, and the Office of Data Management. These key players provide overall direction for data quality initiatives and ensure that strategic plans and infrastructure elements are in place to support the improvement of data quality in the automated systems that support their functional mission.
- Identify data quality projects and develop implementation plans.
- Define, measure, analyze, and improve data quality in selected automated systems on a project-by-project basis. The emphasis is to implement systemic solutions to data quality problems. These solutions may require changes to administrative processes, information systems, PTO policy and procedures, and/or data designs to ensure the quality of data.
- Assess the progress made with respect to: (1) modifying or rejuvenating existing methods to achieving data quality and/or (2) determining whether data quality projects have helped to achieve demonstrable goals and benefits.

Putting the Data Quality Management approach to use within the PTO will improve the quality and utility of data. In the future, data quality management will serve an increasingly important role in facilitating system integration, data migration, and information system interoperability.

REFERENCES

DOD 8320.1-M, *Data Administration Procedures*, March 1994

DOD 8320.1-M-1, *DOD Data Element Standardization Procedures*, January 1993

DOD *Data Quality Management Guidelines* (Draft) April 1996

FIPS PUB 11-3, *American National Dictionary for Information Systems*, February 1991

Redman, Thomas C., *Data Quality Management and Technology*, Bantam Books, New York, 1992

Wang, Richard, Diane Strong, and Lisa M. Guarascio, *Beyond, Accuracy: What Data Quality Means to Data Consumers*, Massachusetts Institute of Technology, Cambridge, MA, October 1994

Zero Defect Data Workbook: Conducting a Data Quality Baseline Audit, QDB Solutions, Inc., Cambridge, MA, 1991

APPENDIX A

Technical Report: Data Quality Analysis Baseline Assessment Report

The following outline illustrates a format to document the baseline analysis for a data quality assessment project. The final report may be similar to this format, or can be prepared as an addendum to this report. The final report should illustrate improvements made, non-quantifiable benefits documented, and cost savings realized.

Table of Contents

I. Executive Summary

II. Background Information of the Information System and Known Data Quality Problems

III. Data Quality Measures

- A. Describe the tables to be analyzed (Table Name, Size, Short Description)
- B. Describe the testing environment, tools used, assigned responsibilities
- C. Level 1 Analysis
  - 1. Description of Level 1 Testing (Describe why each level is being tested)
  - 2. Summarize in tabular format: Tables/columns tested, results for completeness and validity
- D. Level 2 Analysis
  - 1. Description of Level 2 Testing
  - 2. Summarize in tabular format: Tables/columns tested, referential integrity for parent to child, and child to parent
  - 3. Summarize in tabular format: Compliance with cardinality rules if applicable
- E. Level 3 Analysis
  - 1. Description of Level 3 Testing
  - 2. Describe each business rule tested, give number and percentage of results
- F. Level 4 Analysis: Transformation rules
  - 1. Describe transformations required
  - 2. Detail time frames for application of each transformation

IV. Improvement Opportunities

- A. List improvements to accuracy that are immediately achievable
- B. Describe improvements achievable for accessibility, interpretability, and relevancy to data set customers
- C. Explain potential quantifiable and non-quantifiable benefits from the improvements

References

Appendices (may include some or all of the following)

- A. Glossary of Terms
- B. Filter/Test Samples (produced from automated tool)
- C. Exception Reports (reports from automated tool on data quality testing results)
- D. Graphics to illustrate the current problems—may include pie charts, line charts, pareto/control charts

APPENDIX B

Suggested formats for documenting a baseline Data Quality Analysis Report

The following tabular excerpts were extracted from the baseline data quality analysis report for the PTO Corporate Data Mart (now the Financial Subject Area of the Data Warehouse) and are based on the analysis of two samples of daily revenue transactions extracted from the Federal Financial System (FFS). Analysis was made on tables stored in an intermediate data repository prior to transferring the data into the final Oracle data base structures. Data quality analysts are encouraged to use this format. If during your analysis you discover a better way of presenting this material, please submit your format suggestions to the Office of Data Management for incorporation into this instruction during the next document revision.

I. Document the tables to be analyzed:

Data Tables Used in Baseline Analysis

Data Table	Number of Records	Description
DWGJEXT - August 22	1,130	Record per acquisition transaction
DWGJEXT - September 17	727	Record per acquisition transaction
BOC	1,119	Record per BOC code per year
PGMT	14,876	Record per Program Code per year
GLAC	16	Record per GL Accnt Code per year
FUND	63	Record per Fund Code per year
ORGN	9,105	Record per Organization Code per year
RSRC	3,842	Record per Revenue Source Code
TDES	168	Record per Travel Description Code per year

Similarly, document all fields in each table that will be tested. Give table name, column names, data type, and field size.

II. Document Level 1 findings: Completeness and Validity

1. DWGJEXT Table (1,130 records 08-22-96) (727 records 09-17-96)

Data Element	% Incomplete August 22	% Incomplete September 17	% Invalid August 22	% Invalid September 17
Fund Code	0%	0%	0%	0%
Organization Code	0%	0%	0.71%	4.13%
Cost Organization Code	NA	NA	NA	NA
Allocation Organization Code	0%	0%	NA	NA
Program Code	18.58%	28.34%	1.09%	3.84%
BOC Code	0%	0%	0.22%	0%
Budget BOC Code	NA	NA	NA	NA
Revenue Source Code	0%	0%	0%	0%
GL Account Code	0%	0%	0%	0.14%
Ref Doc Trans Code	11.15%	15.41%	NA	NA
Ref Doc Trans Number	11.15%	15.41%	NA	NA
Ref Doc Line Number	11.15%	15.41%	NA	NA
Dollar Amount	0%	0%	NA	NA
Debit Credit Code	0%	0%	0%	0%

For each column analyzed, specify the tests made for validity (domain value set, format, high or low values, etc.). The preferred method for this documentation is to print the filters used in the analysis using the report facility from the automated data quality tool. These pages may be included as an appendix to the baseline analysis.

III. Document Level 2 Findings: Referential Integrity and Cardinality

The analysis for this particular data set for the baseline analysis was accomplished by looking at two distinctive sets of the data. Each data quality analyst must determine what makes the most sense for each project for a baseline assessment. For extremely large data sets, a sampling method may be the most feasible for a baseline assessment. Then, a determination must be made on whether a total analysis of all records in the data set must be accomplished during subsequent analysis and data correction exercises. The emphasis is always on what makes sense for the data set under discussion and the resources available for the effort.

Level 2 Analysis Results

Primary Key Table	®	Foreign Key Table	Key Used	Records Not Found
DWGJEXT Table (1,120 Records 08-22-96)				
DWGJEXT	®	BOC	Budget Fiscal Year + BOC Code	2
DWGJEXT	®	PGMT	Budget Fiscal Year + Program Code	10
DWGJEXT Table (727 Records 09-17-96)				
DWGJEXT	®	BOC	Budget Fiscal Year + BOC Code	0
DWGJEXT	®	PGMT	Budget Fiscal Year + Program Code	20
BOC Table (1,119 Records)				
BOC	®	DWGJEXT August 22 September 17	BOC Code	Unused Codes 370 378
PGMT Table (14,876 Records)				
PGMT	®	DWGJEXT August 22 September 17	Program Code	Unused Codes 5,693 5,749

IV. Document Level 3 Findings: Adherence to Business Rules

Business rules are usually documented with text statements, although business rules may also be documented through printing the filters dealing with business rules directly from the automated tool report print facility. This is the format decided upon for the Corporate Data Mart financial transaction data. More complex data may need a different presentation to clearly state the restrictions on the data imposed by business uses.

Business Rule Results for DWGJEXT Table

Note: Records out of conformance are documented as "Number/Number" where the first number is the August 22nd data and the second number is the September 17th data.

3050 - BOC Code exists & DocTransCode = CR, CT

If the Document Trans Code is "CR" or "CT" then the BOC Code must be blank.

Records not in conformance: 0/0

3060 - Budget BOC Code exists & DocTransCode = CR, CT

If the Document Trans Code is "CR" or "CT" then the Budget BOC Code must be blank.

Records not in conformance: 0/0

3065 - 1st 2 chars BOC CODE <> BudgetBOC

The first two characters of each BOC Code must match exactly the first two characters of the Budget BOC Code.

Records not in conformance: 0/0

3230 - RefDocTransCd exists & GL Acct = 5211, 4700

If the GL Account Code is "5211" or "4700" then the Ref Doc Trans Code must be blank.

Records not in conformance: 56/26

3240 - RefDocTransNum exists & GL Acct = 5211, 4700

If the GL Account Code is "5211" or "4700" then the Ref Doc Trans Num must be blank.

Records not in conformance: 56/26

V. Document Level 4: Define transformation rules and the time frames for application

Transformation rules are defined with SQL statements. Time frames for application are defined in terms of where in the information system life cycle application will be made.

VI. Specifying Improvement Opportunities

The baseline report is not complete without specifying improvement opportunities and suggested times for implementation of these suggestions.

Improvement Recommendations

The Corporate Data Mart data quality issues revealed in the baseline assessment suggest that a plan of action to improve data quality will require some or all of the following steps:

1. Organize a one-time data clean-up effort to improve the completeness, validity, and consistency of data within all records. The baseline system can be used to provide a full inventory (work list) of these types of problems.
2. Solicit critical missing data from alternative sources (e.g., other data bases, manual files, etc.).
3. Organize an effort to research and resolve the missing records reflected in the referential integrity problems. The baseline system can be used to provide a suspense list of missing records by primary key.
4. Initiate enhancements and modifications for the Corporate Data Mart source processing systems to strengthen the data field editing and record control functions to prevent future deterioration in data quality.
5. Develop a periodic audit process that will review the data content of a significant sample of Corporate Data Mart data records against their sources.

Monitoring Recommendations

Concurrent with implementing the above plan of action, a selective set of Corporate Data Mart data quality issues should be incorporated into an Corporate Data Mart Data Quality Monitoring System. The purpose of that system will be to analyze Corporate Data Mart data on a regularly scheduled basis and produce metrics of the current data quality condition as well as trend reports and graphs to show the changes in data quality over time. While the monitoring system will use additional functional features of QDB Analyze™ (now a Prism tool) not needed during the baseline assessment, most of the analytical techniques developed can be converted directly to the new monitoring system.

Attachment 8

UNITED STATES
PATENT AND
TRADEMARK OFFICE

Information Technology Standards and Guidelines Program

Data Management

Technical Standard and Guideline IT-212.02-05

February 2002

Executive Summary

This Technical Standard and Guideline (TSG) explains how to prepare a Data Management Plan for an Automated Information System. A Data Management Plan guides data management in Automated Information Systems by specifying responsibilities, approach, products, required tasks, and documentation for the systems.

This guideline contains content and format requirements for a Data Management Plan. The Chief Information Officer of the United States Patent and Trademark Office publishes this guideline. This guideline applies to all Automated Information System development projects. Compliance with this guideline is required unless the Chief Information Officer grants a waiver.

The Data Management Plan is based on the *Life Cycle Management for Automated Information Systems* manual. The Data Management Plan also supports the requirements of the United States Patent and Trademark Office policy on Data Administration, effective October 16, 1995, and the Paperwork Reduction Act.

1. PURPOSE. To guide data management for Automated Information Systems and establish standards for data management plans.

2. AUTHORITY. This publication is published under the auspices of the Chief Information Officer (CIO), United States Patent and Trademark Office (USPTO), in accordance with the USPTO Data Administration Policy, Office Administrative Directive, Automation and Automatic Data Processing 212-01, dated October 16, 1995.

3. APPLICABILITY. This guidance applies to all USPTO personnel responsible for Automated Information Systems Data Management planning, and their supporting contractors.

4. SUMMARY OF CHANGES: This TSG applies to all Automated Information Systems projects. This TSG supercedes the previous Data Management TSG, October 1995.

5. SCOPE

   a. Compliance. Compliance with the provisions of this document is required unless a specific waiver is authorized.

   b. Waivers. Waivers to the provision of this publication will be authorized only by the CIO, on a case-by-case basis. Waiver authorization may be delegated to the Director, Office of Data Management.

6. RECOMMENDATIONS. Recommendations concerning the contents of this technical publication should be forwarded to the USPTO OCIO Software Engineering Process Group (SEPG) and the Office of Data Management.

7. APPROVAL. The Data Management Plan shall be approved jointly by the Project Manager, the System Development Manager and the Director of the Office of Data Management.

__SIGNED____________________
Douglas J. Bourgeois
Chief Information Officer

February 12, 2002____
Date Signed

Record of Changes

CHANGE NUMBER	DATE OF CHANGE	DATE RECEIVED	DATE ENTERED	SIGNATURE OF PERSON ENTERING CHANGE

Table of Contents

1 GENERAL

1.1 Introduction

This *Data Management* Technical Standard and Guideline (TSG) provides detailed instructions for the preparation of data management plans. It applies to all United States Patent and Trademark Office (USPTO) Automated Information System (AIS) projects, as outlined in the *Life Cycle Management for Automated Information Systems* (LCM-AIS) manual.[1] Its provisions apply to all development, migration, re-engineering, maintenance, and retirement efforts for any major automated information system and limited infrastructure projects.

Guidance for AIS data modeling, data naming convention, and data element standardization do not appear in this TSG. Guidance for those activities can be found in the *Detail Design Document* and *Data Element Naming Conventions and Standardization TSG*, IT-212.03-13. Records management guidance can be found in the *United States Patent and Trademark Office Comprehensive Records Schedule.* The Data Administration Division of the Office of Data Management (ODM) is responsible for AIS project records management support for electronic, paper, and other records. Consult ODM for guidance on electronic records management and the procedures for managing Standard Generalized Markup Language and eXtensible Markup Language document resources in the *Standard Generalized Markup Language (SGML) and eXtensible Markup Language (XML) Resource Management Guidelines Technical Note, IT-212.2-05, TN01.*

1.2 Concepts and Definitions

Data management planning is an important element of system life cycle activities. It begins during the earliest phase, proceeds as requirements are defined and software is implemented, and continues until the automated system is terminated or replaced. The data management activities performed during the system development life cycle are based upon the following basic principles.

Data is recognized as a valuable resource.

Data is collected, stored, safeguarded, and used to support agency missions and business processes and decisions, making accurate and timely data an important corporate resource.

Data is defined separately from the technology used to collect and store it.

Business area data requirements are recorded clearly before designing automated data collection and storage methods, so that program needs are understood and recorded.

Accurate information about data is essential.

[1] The *Life Cycle Management for Automated Information Systems (LCM-AIS)* may be found at http://ptoweb/ptointranet/cio/index.htm.

Effective management of data collected by the business area requires that accurate information about data (metadata) be kept.

Common data management guidelines, methods, and tools are used.

A common approach to defining, modeling, designing, and documenting data improves data quality and makes it easier to share data among systems and offices.

A data architecture is developed and maintained.

The USPTO common data architecture is the high-level structure and organization of USPTO data. The creation of a common data architecture across the USPTO enterprise supports data sharing and information system interoperability. It defines USPTO data in a common context, addresses data quality issues, and fosters information understanding throughout the enterprise. The USPTO common data architecture is comprised of the Enterprise Data Model, data element naming conventions, standard data elements, and the Enterprise Information Repository.

1.3 Data Management Objectives

This TSG provides guidance for preparing the Data Management Plan. The objectives of the Data Management Plan support overall USPTO data policy objectives. These include:

- Recognize and promote the importance of data and information as valuable resources. This can only be achieved by proper management of the creation, use, storage, documentation, and disposition of data.

- Promote data consistency and standardization throughout the organization by developing standards for data element names, definitions, values, formats, metadata, and documentation in the Enterprise Information Repository and in data bases.

- Minimize duplication in collecting, processing, storing, and distributing data.

- Encourage and facilitate data and information sharing among USPTO business areas, the Department of Commerce, other Federal agencies, and the intellectual property community world-wide.

- Improve the quality, accuracy, and integrity of shared data resources.

- Improve data administration and access to metadata with appropriate new and existing methods, tools, and technologies.

- Reduce the cost and time to implement automated information systems.

- Implement single point of entry for data.

1.4 Context of Data Management Plan in the AIS Life Cycle

The Data Management Plan components conform to the USPTO methodology for life cycle management for an AIS. Data management planning begins in the Concept Phase and continues through the Operations Phase. The Data Management Plan is written during the Concept Phase, and is approved and placed under configuration management at the end of the Detailed Analysis and Design Phase. Change control authority to the Data Management Plan requires concurrence of System Development Management and the Office of Data Management from this point in the life cycle forward. The System Development Manager is responsible for any impact that changes to the Data Management Plan may have on the rest of the project, such as data and activity modeling, and testing. The Data Management Plan is an evolutionary document and is updated as needed during each life cycle phase.

1.4.1 Prior Activities

Data management planning begins early in the Concept Phase upon the development and approval of a Business Case and immediately following initiation of the System Boundary Agreement.

1.4.2 Concurrent Activities

In the Concept Phase, the Data Management Plan is written concurrently with other AIS documents as outlined in the Quality Assurance Plan (QAP). The Data Management Plan establishes the framework for data management development related activities in the Detailed Analysis and Design Phase. This includes data management approach, data requirements gathering, stewardship roles and responsibilities, data element identification, metadata management, model management, data management tools, records management (electronic, paper, and other records), expected information collection burden, and data privacy.

In the Detailed Analysis and Design Phase, the Data Management Plan is revised concurrently with other AIS documents to confirm the data management related activities for this phase, as well as those data management activities outlined in the Development Phase.

In the Development Phase, data management occurs concurrently with preparation of other AIS documents as outlined in the Quality Assurance Plan (QAP). It establishes the framework for subsequent Deployment Phase processes, including testing, transition, data conversion, and records management (electronic, paper, and other records).

In the Deployment Phase, data management occurs concurrently with the validation of the production environment. It establishes the framework for data base management, data integrity, and records disposition concerns during the subsequent Operations processes.

1.4.3 Follow-On Activities

Data management planning is an iterative process throughout the entire life cycle encompassing follow-on activities. In each phase, the Data Management Plan may readdress topics covered during earlier phases to refine concurrent processes.

1.5 List of Products

The resulting products required from this TSG are the Data Management Plan and, when applicable, the Data Conversion Plan. The Data Management Plan describes the data management approach that will be used and defines data related activities that will be completed for the AIS project. The Data Conversion Plan describes the details of transforming data from its original source to the newly designed target data base. A sample outline of the Data Conversion Plan is in Appendix G.

2 TASKS AND RESPONSIBILITIES

2.1 Office of Data Management

The Office of Data Management consists of the Data Administration Division (DAD) and the Data Base Administration Division (DBAD). The Data Administration Division's major tasks are performed during the Concept and Detailed Analysis and Design Phases of the project's Life Cycle Management, tapering off gradually near the end of the Development Phase. The Data Base Administration Division plays a minor role during the early phases of the project's Life Cycle Management, but actively participates and performs major tasks during the Development, Deployment, and Operations Phases of the system. The Data Base Administration Division should be consulted prior to the completion of the Detailed Analysis and Design Phase, before the data base design is completed. In addition, the Office of the Director administers the Enterprise Information Repository and the XML Resource Repository.

2.1.1 Data Administration Division

The Data Administration Division is responsible for ensuring the most cost-effective organization and use of an enterprise's data resources. The Data Administration Division is ultimately responsible for supporting AIS projects with data management support. This includes data management plan guidance, data modeling, and data element naming and standardization and facilitating the sharing of corporate data and information. The Data Administration Division is also responsible for supporting AIS projects with records management support for electronic, paper, and other records. This includes implementing sound records management and information collection practices that ensure compliance with federal laws and regulations and assisting business areas to operate more efficiently. The Data Administration Division is also responsible for supporting AIS projects with electronic records management support for storing records for effective management of the associated electronic records. The Data Administration Division responsibilities include, but are not limited to, the following activities.

- Prepare, implement, and manage data administration policies, procedures, rules, standards, and guidelines;

- Develop and maintain a consistent data architecture, including a logical Enterprise Data Model and logical data models of business areas, and support development and validation of physical models for automated systems;

- Enforce data element naming conventions on logical data models and physical data bases;

- Design, implement, and manage the data standardization process and the supporting Enterprise Information Repository of metadata;

- Prepare and approve data management plans, data models, data naming, and standard data elements;
- Manage the Data Stewardship program;
- Manage the Data Quality program;
- Advise data stewards on data quality assessments and improvements;
- Facilitate business process re-engineering through the identification of opportunities for shared data;
- Administer the USPTO records management and electronic records management programs;
- Administer the Vital Records Program;
- Administer the USPTO information collection burden program under the Paperwork Reduction Act; and
- Carry out the objectives of the Data Management policy, whether explicitly stated or not.

2.1.2 Data Base Administration Division

The Data Base Administration Division, Office of Data Management, stores, secures, and maintains data bases. This office ensures that all data bases and operational systems are running at optimum performance while providing support for new development and AIS projects. The responsibilities of the Data Base Administration Division include the following activities:

- Meet and consult with development teams, provides vendor and technical support for development teams, and create physical data bases;
- Support AIS projects by reviewing proposed changes; troubleshooting; and assisting with retrieval, web tools, special changes, strategic planning, and end user support;
- Provide support services for developing automated information systems, such as requirements analysis, data base design, and implementation and maintenance strategies for data base applications;
- Support systems programming with software maintenance, system monitoring, software management, and in-house documentation;
- Support operational maintenance with operational readiness, data base management, backup/recovery and security; and

- Monitor licensing compliance and assists the Help Desk with training and interpretation of error conditions.

2.2 Data Management Overview

This section describes the tasks and responsibilities of the USPTO employees and supporting contractors for AIS data management. Data management includes:

- Preparing the Data Management Plan;
- Defining the data management approach; and
- Defining and supporting the data management tasks.

Preparing the Data Management Plan begins with an interview with the project's System Development Manager. Initial discussion between the DAD staff and the SDM should reveal high-level information about the project methodology, tools, system architecture, data, and key players. Discussion should reveal:

- How the requirements and data are collected;
- Where the data resides and who will manage it;
- Who has programmatic control over the data;
- Who has business knowledge of the data;
- If there are any new data elements introduced or changes to existing data elements;
- If the current system's legacy data elements have not been documented or validated in the Enterprise Data Model;
- If the Extensible Markup Language (XML) techniques and tools will be used;
- If the system will be using a Commercial-Off-The-Shelf package, Object-Oriented tool or Integrated-Computer Aided Software Engineering tool;
- How the system will address records management (electronic, paper, and other records) requirements; and
- How the data will be shared with other organizations or systems.

The DAD staff will review other documents for the project such as the Concept of Operations, Business Case, System Boundary Agreement, Requirement Specifications, and the Quality Assurance Plan. The tailoring agreement that contains required and waived Life Cycle Management documents is part of the QA Plan. The Data Management Plan is part of the required Life Cycle Management documentation. The Director of the Office of Data Management holds the authority for the waiver of the Data Management Plan.

Table 2.1 provides a summary of roles and tasks for the data management planning process and each USPTO office responsible for its execution. A more comprehensive project specific listing of roles and functions should be included in the Project Management Plan.[2] In Table 2.1, the same person may perform multiple functions.

Table 2.1 Summary of Data Management Activities by Roles and Functions

FUNCTION ⇒ ROLE⇓	Data Planning	Prepare and Review Data Management Plan
Program\Project Management	Consult with Data Administration on the data management approach and support the identification of data stewardship and data quality	Review and assist as needed in the development of the Data Management Plan
System Development Management	Provide support for data management development activities Coordinate data management activities for compliance with Data Management Plan Comply with Data Management Plan	Review and submit Data Management Plan for review to Quality Assurance, Program Management, Configuration Management, System Architecture and Engineering, Operations, Testing, and End-Users
Office of Data Management	Provide support in using the Enterprise Information Repository	Conduct impact analyses, train, and generate special reports
Data Administration	Prepare Data Management Plan Evaluate and select data approach, methodology, and tools Provide data administration expertise for the preparation of Data Management Plan Provide XML expertise for the preparation of XML DTD/Schema development Evaluate data resources and acquisition, data quality management, records management (electronic, paper, and other), and information collection burden Provide support for the development of the logical data model Provide support for the physical data model ensuring adherence to data element naming convention and enforcement of referential integrity Provide support for standardization of data element	Prepare, Update, and Submit Data Management Plan to System Development Manager Evaluate and approve Data Management Plan for compliance with data administration policies and procedures Evaluate and approve XML DTD/Schema for compliance with SGML/XML Resources Management Guidelines

(Table 2.1 is continued on the next page.)

[2] Refer to the LCM-AIS manual for a description of the Project Management Plan.

Table 2.1 Summary of Data Management Activities by Roles (Continued)

FUNCTION ⇒ ROLE ⇓	Data Planning	Prepare and Review Data Management Plan
Data Base Administration	Provide data base administration expertise in planning for development and maintenance of physical data base, including operational impact analysis, data model analysis, implementation impact analyses Plan and schedule development and operational data base implementation, and coordinate with SDM and OSAE regarding data capacity Advise on DBMS and support tools	Evaluate compliance to technical standards for physical maintenance of data resources
Quality Assurance (QA)	Evaluate Data Management Plan for compliance with LCM	Review Data Management Plan
Configuration Management (CM)	N/A	Place Data Management Plan under CM
System Architecture and Engineering	N/A	Review Data Management Plan for compliance with Technical Reference Model and Information Technology infrastructure
Operations	Provide support for data management deployment activities	Review Data Management Plan
End-User Involvement	Participate in data stewardship assignments, data resources, and acquisition Perform data quality monitoring	Review Data Management Plan

2.3 Concept Phase

The Data Management Plan is written during the early part of the Concept Phase. In the Concept Phase, the Data Management Plan will address the project data management approach, data stewardship, data management tools, metadata documentation products, and additional data management activities.

2.3.1 Data Management Approach

The data management approach has a major influence upon the success of an automation project. The data related activities, products, and decisions that must be addressed during the system life cycle constitute the data management approach. The approach includes the degree of rigor to be followed when performing these activities and the level of formality to be used when documenting data-related life cycle products and decisions.

Implementing a data management approach is one key to the project's success. If the approach does not address data management issues, the risk of time and cost overruns for the project will increase, as will maintenance costs for the completed system and its data.

There are two criteria to determine the data management approach: the degree of data sharing and the AIS project type. Data sharing includes use of one information system's data by a second system, and utilizing the same data for multiple functions within a single information system. There are three basic ways of sharing automated data:

- Downloading/uploading information from a data store;
- Creating/replicating an external copy of a file; and
- Creating and using shared data bases.

If data sharing exists, the data management approach should include all data management activities. Following this type of approach will minimize unexpected, negative impacts upon the system and the programs it will support. Use of standardized data elements is one way of facilitating data sharing.

If an Automated Information System project is considered a stand-alone system with no data sharing, a Data Management Plan is helpful in addressing records management (electronic, paper, and other records) issues, data quality, information collection burden; ensuring the logical view of data is clear and completely addresses all business requirements; and ensuring the physical design of the data base incorporates data integrity.

2.3.1.1 Automated Information System Projects

A second criterion that influences the data management approach is the strategies used n developing an AIS. The strategy determines the required data activities and products. These include, but are not limited to, the following: Commercial-Off-The-Shelf Application, Government-Off-The-Shelf Application, Integrated-Computer Aided Software Engineering Based, Object-Oriented Based, Multiple Phased Project, Mixed Solution, and Multiple Related AISs.

- Commercial-Off-The-Shelf Application Project
  A Commercial-Off-The-Shelf (COTS) application project requiring no supplemental code (e.g., scripts, macros, command files, configuration files, etc.) may follow a modified data management approach. No physical data base design is required. If the data base is Oracle then it should be imported into the Enterprise Information Repository. A mapping matrix is required showing all logical attributes and what they map to in the physical data base (as feasible).

Although a modified data management approach may be used for COTS, it is strongly recommended that the creation of a logical data model be considered. In this scenario, the logical data model is compared to the data contained in the potential COTS packages. A major factor in COTS package selection is the degree to which the logical data model attributes, entities, and business rules are aligned with the potential COTS. This is the major determinant in evaluating how well a COTS package meets the business requirements. Contact the Data Administration Division for instructions on tailoring the data management approach. Examples of USPTO COTS projects include the following: Enterprise Asset Management System, Patent and Trademark Assignment System, and Information Technology Facilities Management System.

- Government-Off-The-Shelf Application Project
  A Government-Off-The-Shelf (GOTS) application project requiring no supplemental code may follow a modified data management approach. No physical data base design is required. If the data base is Oracle then it should be imported into the Enterprise Information Repository. A mapping matrix is required showing all logical attributes and what they map to in the physical data base (as feasible). Similar to COTS, it is strongly recommended that a logical data model be created. The logical model is used to evaluate whether the GOTS meets the business requirements. Contact the Data Administration Division for instructions on tailoring the data management approach. An example of an USPTO GOTS project is the Office of Human Resource System.

- Integrated-Computer Aided Software Engineering (I-CASE) Based Project
  A project that plans to use the I-CASE based tools should include all data management activities. Products such as the logical data model and the physical data base design may be produced automatically from the I-CASE tool by the System Developer and accepted as a data management product. Products such as the logical data model should be stored in the USPTO Enterprise Information Repository. Examples of USPTO I-CASE projects include the following: Patent Application Location and Monitoring (PALM) Migration Pre-Exam Subsystem, PALM Examination and Post-Examination Subsystem, and Revenue Accounting and Management System.

- Object-Oriented (OO) Based Project
  A project that plans to use the OO based tools should include all data management activities. Products such as the Use Case and Class diagrams may be produced automatically from this tool by the System Developer and accepted as a data management product. An example of OO Based project is Tools for Electronic Application Management.

- Multiple Phased Project
  When a project is to be implemented in more than one phase, the Data Management approach is determined by the amount of information known about the phase to be implemented. The Data Management Plan may change as more information is revealed throughout the Life Cycle Management phases. New versions of the Data Management Plan may be necessary

as additional phases of the project are introduced. Examples of USPTO multiple phase projects are: Trademark Electronic Application Submission, Office of Human Resource System, and Trademark Image Capture and Retrieval System.

- Mixed Solution
  A project that plans to use a combination of either I-CASE, OO, COTS, and/or custom software should include all data management activities. All metadata products (e.g., logical and physical data model, object model, data base schema) shall be stored in the USPTO Enterprise Information Repository. Contact the Data Administration Division, Office of Data Management, for guidance. Examples of USPTO mixed solutions projects are: Enterprise Address Data Component and Office of Finance Imaging System.

- Multiple, Related AISs
  When multiple, closely related AISs are to be developed and deployed, it is possible that a single subject area Data Management Plan may be developed, addressing all data management activities that are applicable. The decision to select this option is based on complexity and manageability and will be made by the Office of Data Management. Examples of USPTO multiple related AIS projects are: Pre-Grant Publication, and Tools for Electronic Application Management.

Regardless of project type, the electronic records management requirements still apply unless waived by the Chief Information Officer. For additional details on electronic records management considerations, consult the Electronic Records Management Team Leader.

2.3.1.2 Approach Selection

Depending on the degree of data sharing and the project type, determine the data management approach to use for the project. Choose the tasks, products, and activities to be included in the data management approach. A primary objective of every automation project is to provide accurate and consistent data to the business users. Record the data management approach in the Data Management Plan early in the Concept Phase and refer to the Plan at the beginning of each phase, revising it as necessary.

2.3.2 Data Stewardship

Another major activity that the Data Management Plan addresses is the parties responsible for data. Data stewardship is defined as "...the willingness to be accountable for a set of business information for the well-being of the larger organization..."[3] The data stewardship program consists of establishing teams of people (both business users and CIO staff) that have a vested interest in the content and/or structure of particular classes of data and who will assume

[3] English, Larry P., *Improving Data Warehouse and Business Information Quality*, John Wiley and Sons, Inc., New York, 1999

responsibility for the preservation and quality of that data. The data stewardship program is a means to leverage the cooperation already established between CIO and the business users. It provides a means by which the data stewards can work together to ensure that data is of high quality and is useful to all who need the data to conduct their business at the USPTO. Data stewardship is a proactive approach to improving data quality and data sharing.

The goal is to simplify the flow of program data. Data should be created once and used often. Replication of data should be planned. However, currently the flow of program data is often lengthy and complex, as data is collected at various locations. Managing the complex activities, responsibilities, and relationships that arise from these data flows requires a method of determining which organizations involved in the data flows are responsible for which data-related activities. One reason that redundant and inconsistent data exists is due to the low confidence in the accuracy of data, even if that opinion is unfounded. One of the main goals of information stewardship is to improve the quality of data. As data become more accurate, reliable, timely, and complete, data sharing should increase and redundant and inconsistent data should be reduced.

2.3.2.1 Data Stewardship Roles and Responsibilities

The USPTO's data stewardship program consists of three levels of data stewardship: Business, Operational, and Technical stewards along with the Stewardship Quality Council.

- **Business Area Steward**
  - Ultimately accountable for the business data
  - Assigns the Operational Data Steward
- **Operational Data Steward**
  - Accountable for the content and business rules surrounding the business data
  - Accountable for identifying and defining electronic records from a business perspective including defining and initiating the archival processes
- **Technical Information Steward**
  - Accountable for the technical infrastructure supporting the processing of the data requirements within an AIS
  - Accountable for the management of electronic records and describing where and how to point at the subject records for the archival processes

Along with:

- **Stewardship Quality Council**
  - Resolve data related issues and data conflicts

As caretakers of specific business area data and electronic records, data stewards:

- Represent their business area in enterprise-wide data activities;

- Participate in the development, validation, and approval of data models and standard data elements involving their business area, assisting the data administrator as required;
- Participate in electronic records administration in order to deploy an electronic record keeping system where records are collected, organized, and categorized to facilitate their preservation, retrieval, use, and disposition;
- Work with the Office of Data Management to assess and improve data quality; and
- Support an enterprise-wide view of data sharing.

The data stewardship guidance presented in this section has the following objectives:

- Facilitate the assignment of responsibilities for data definition, collection, processing, storage, use, and disposition when systems and data bases are being built;
- Notifiy the USPTO Records Officer of system content and purpose, providing useful descriptions to facilitate official disposition instructions for the system and its records, from the National Archives;
- Ensure data meets mission and business area requirements by assigning accountability for high quality data and electronic records;
- Ensure that data definition, collection, processing, and storage methods within the organization's systems conform to applicable guidelines;
- Facilitate data sharing and reuse by clarifying roles and responsibilities involved in the definition, collection, processing, storage, and use of data; and
- Help the system developer ensure that the standard naming conventions are applied and standard data elements are used.

A discussion of each data stewardship role follows:

Business Area Data Steward

The same organization with overall responsibility for a business area's performance is responsible for ensuring that the quality of data required to support the business area is defined, collected, processed, stored, and presented in a timely and cost-effective manner. The main function of the Business Area Data Steward is to assign operational data stewards for all business functions within their organization. If a data element is used by more than one project, multiple data stewards will be assigned so that any changes to the data element can be properly coordinated.

Operational Data Steward

The Operational Data Steward is the subject matter expert from the organization or function who is responsible for the definition and collection of data and who exercises programmatic control over electronic records. Since the level to which an organization understands its data directly correlates to the level of success of any AIS, it is the role of the Operational Data Steward to define the metadata or characteristics about the data and electronic records used in their business functions, along with the derivation rules and the formats to be used for data derived from other data elements, along with security requirements. When multiple functions or organizations use the same data to support important program functions, a joint data definition effort is organized. In defining and collecting data, the Operational Data Steward(s) will be concerned with the following items:

- MEANING - what is the business definition of the data item (e.g., name, description, data type, length)
- CONTENT - what valid values, ranges, and formats the business expects
- BUSINESS RULES - how does the business use the data and what are its relationships with other data
- UTILIZATION - What are the appropriate federal and internal regulations and standards that must be met
- SOURCE - where in the business process did the data come from
- TARGET - where does the data go next
- RETENTION - how long must the data be available
- DATA SENSITIVITY - should the data be protected from unauthorized disclosure, alteration, or destruction
- ISSUES - are there any known problems or concerns about the data
- THRESHOLD OF ACCEPTABILITY - determine the minimum level of quality or integrity the data must maintain
- DATA QUALITY- does the data quality meet the business information needs

Technical Data Steward

The organization responsible for storage and processing of data is the Technical Data Steward. The functions carried out by the Technical Data Steward include those that have traditionally been performed by Automated Data Processing (ADP) organizations, such as the System Development and Maintenance Managers, Data Base Administrators, and Data Maintenance Branch/Operations staff. During the development life cycle, this stewardship role will be assigned to the system development manager until the system is turned over to the operating organization. The Technical Data Stewards are responsible for the storage and processing of data. They are responsible for the following items:

- Maintain physical custody or direct control of the data, software, and other components used to store, process, communicate, and present data;
- Ensure the physical integrity of data;
- Safeguard the storage media;
- Carry out data sampling and data problem resolution;
- Act as Records Management contact; and
- Act as Paperwork Reduction Act contact.

Since both the Operational and Technical Data Stewards are responsible for ensuring that the data administration standards are met when defining and documenting data, the stewards will rely on the procedures contained in the *Data Element Naming Conventions and Standardization Technical Standard and Guideline, IT-212.03-13,* when defining data. The central information repository should also be reviewed for already existing standard definitions of data.

As an example, for the USPTO Standard Country information, the following data stewardship roles exist.

Table 2.2 Sample Data Stewardship Roles

Business Area Data Steward	Operational Data Steward	Technical Data Steward	USPTO Organization	AIS
Bob Saifer			International Liaison Staff	
	Ed Rishell		International Liaison Staff	
		Horatious Tanyi	Office of System Development and Maintenance	PALM MG Shared Objects
		Susan Shifflett	Office of System Development and Maintenance	PTAS and AHD
		Lana Chow	Office of System Development and Maintenance	ACTS
		Kathryn Tindle	Office of Data Management	

Stewardship Quality Council
The Stewardship Quality Council meets periodically to discuss data related issues of interest. Membership will consist of a Chair (Director of Office of Data Management); Vice Chair (Manager of the Data Administration Division); Coordinator (Data Administration Division Team Leader); and the Business Area, Operational, and Technical Data Stewards. The level of involvement of the council will vary depending on the volume and complexity of data issues. The Chair, Vice Chair, and Business Area Data Managers will only be involved during conflict resolution.
In addition to the data stewardship roles, the Data Management Plan will document the following roles in a system development project:

Program Sponsor
The Program Sponsor is responsible for overall project management, makes resources available to support the project, defines and validates customer requirements, and reviews progress at each LCM milestone. The Program Sponsor consults with the Office of Data Management in the selection of the data management approach. The Program Sponsor will assign the Project Manager.

Project Manager
The Project Manager is responsible for overseeing the complete effort to achieve implementation of the project. The Project Manager provides daily direction, coordination, and control for all aspects of the design, development, and deployment of the system subject to the technical direction of the Office of the

CIO and business direction of the Program Sponsor. Utilizing matrix management, the Project Manager directs the day-to-day activities of all members of the project team and ensures that all tasks and functional roles for data management planning are performed adequately in order to provide a system of sufficient quality to support program missions.

System Development Manager
Appointed by the CIO, the System Development Manager is responsible for designing, developing, and deploying an AIS under the business direction of the Project Manager. The System Development Manager ensures that the project is consistent with the agency's strategic information technology plans and is managed according to sound life cycle management principles and practices.

Maintenance Manager, Data Base Administrators, and/or Computer Operations Staff
The Maintenance Manager, Data Base Administrators, and/or the Computer Operations staff are responsible for the operation of the AIS or infrastructure system. The Maintenance Manager is responsible for the day-to-day operations of the system and for ensuring that the operational system remains consistent with the agency's strategic information technology plans.

The Data Base Administrators are responsible for ensuring that the data is available for operations as outlined in the Operational Support Plan.

The Computer Operations staff is responsible for ensuring that the infrastructure required to support the system is available in accordance with the requirements described in the Operational Support Plan.

Primary User(s)
The organization or function with the most important requirement to collect, store, and process data to perform a current or future business area function is the primary user. Sometimes the data steward organization designates the primary user, as the definer of the data the organization requires. Primary user organizations support user testing of systems during the life cycle, and ensure on-going data quality for the system data once the system is operational. If it is impossible to select a single primary user organization from among several users of the same data, then a joint data definition effort will probably result. The primary user organization is often, although not always, the data steward organization.

Ancillary User(s)
The ancillary users use data to perform business area functions, and report results to management, the Congress, and to others outside the agency. Unlike the

primary users, ancillary users must rely upon others to define and allow them access to the data.

Records Officer
The Records Officer records the dispositions (i.e., maintain, update, archive, delete or destroy) of the system software, documentation, data, output records, and backups in the USPTO Comprehensive Records Schedule. The USPTO Records Officer, Office of Data Management, serves as the Records Management contact for all projects and will oversee and coordinate the disposition scheduling process with the Operational and Technical Data Stewards.

Records Coordinator
The Records Coordinator is a person designated by the Program Office to be the point of contact for assisting with the actual disposal of records. The Records Coordinator will also assist in the retrieval of records currently archived to NARA.

2.3.2.2 Data Stewardship Implementation Activities

During the Concept Phase, contact is established between the data administrator and the project's management team to discuss the scope of the project's application and the general types of information anticipated for the application. If the project management team and the data administrator determine that multiple data steward organizations will be involved in a project, plan to involve all of these organizations beginning in the Concept Phase. Since implementation of stewardship at the data base or project level is not feasible when multiple organizations are involved, record the steward for each major function within each organization involved in the project. Ensure that Business Area, Operational, and Technical Data Stewards are recorded for all data elements. Ensure primary and ancillary users and records coordinators are recorded for the system.

When one organization defines, collects, and uses a set of data, that organization is the probable data steward. However, when data definition, collection, and use are split between multiple organizations, one faces a more difficult problem in determining stewardship. When this occurs, both of the primary user organizations should be selected as the data steward. When stewardship of data is shared between organizations, the organizations must coordinate when any permitted values or data structure is going to change so that the usability of the data is preserved for all users of this data. The Data Administration Division facilitates that coordination.

Concept Phase Data Stewardship Implementation Activities

- The Project Manager and System Development Manager will identify the organizations that will likely be the information steward organizations for the data the project requires.

- The Project Manager will assume the responsibilities of the Business Area Data Steward for the project. The Project Manager and System Development Manager will appoint individual(s) to assume the responsibilities for the Operational Data Steward. The System Development Manager will assume the responsibilities of the Technical Information Steward for the project.

- The Data Administration Division works with the appointed Operational Data Steward(s) to determine the Primary User(s), and Ancillary User(s). The Operational Steward will be involved in identifying data entity types as the project management team performs data modeling. Detailed information on data element naming is in the Data Element Naming Conventions and Standardization TSG.

- After the project management team has completed the data entity type and initial entity list, the Operational Data Steward assists in defining each data entity's meaning within the scope of the mission.

2.3.3 Data Management Tools

The automated tools that will be used during the project's life cycle to support data management activities need to be recorded in the Data Management Plan document. Explicit plans for managing the flow of metadata (information about data) between methods and tools through the life cycle should be documented. These tools include data modeling tools, data base management systems, records management (electronic, paper, and other records) tools, and information repositories. Explicitly identify any data management software to be used during the project's life cycle. Consult the USPTO's Technical Reference Model (TRM) for a current list of approved USPTO data management tools.

2.3.4 Metadata Documentation Products

This section describes the essential metadata documentation activities that must be performed during the system life cycle. While documentation is required of other life cycle products, this TSG covers only the essential metadata documentation of data requirements, physical data base designs, and production data base structures. The documentation must be completed to support later phases of the life cycle, reduce maintenance costs, and provide an audit trail from requirements to production data bases. Planning for metadata management is initiated in the Concept Phase. Careful management of the project Data Management Plan document will allow tracking of the project's data requirements through the production data base.

The System Development Managers need to plan and monitor the project's collection, use, and transfer of metadata throughout the system life cycle. Failure to do this task could delay the project, increase the cost of the project, or cause a data base to be implemented that does not meet requirements. Consult the Data Administration Division, Office of Data Management concerning the Enterprise Information Repository and XML Repository to support the project.

- High-Level Logical Data Model
  A high-level logical data model is required for all AIS projects. Plans to develop logical models using Information Engineering Methodology (IEM) technique should be initiated during the Concept Phase. The Enterprise Data Model (EDM) must be reviewed to identify potential entities that are required for the AIS. A subset of the required entities should be extracted or copied from the EDM. This subset model shall form the foundation for data modeling in subsequent life cycle phases. The logical data model should contain at a minimum entities, entity definitions, and relationships. Entity-Relationship modeling is to be used during the Concept Phase to maintain the integrity of the Enterprise Information Architecture. The *Detail Design Document TSG* contains specific guidelines on logical modeling techniques.

- SGML/XML Resources
  Any project developing a system that processes content and uses XML to do so, will work with the XML Registrar or XML Technical Working Group (TWG). During the Concept Phase, categories (the structure used to store resources in the XML Resource Repository) are established. For details on XML resources, please see the *Standard Generalized Markup Language and eXtensible Markup Language Resource Management Guidelines Technical Note, IT-212.2-05: TN01.*

- Other Metadata Products
  There are other metadata documentation products that may be required for an AIS project such as the data element standardization worksheet, the XML element and logical data element mapping matrix, and the physical to logical data element mapping matrix. Reference Appendix E and F, and *Standard Generalized Markup Language and eXtensible Markup Language Resource Management Guidelines Technical Note, IT-212.2-05: TN01.* Consult the Data Administration Division for more information to tailor these needs.

2.3.5 Additional Data Management Activities

Records Management

Records Management is an integral part of AIS data management. It implements the USPTO's compliance with requirements of the Federal Records Act. The most relevant of those requirements mandate that the head of each Federal agency shall establish and maintain an active, continuing program for the efficient management of agency records. The vehicle for the management of agency records is an up-to-date records disposition schedule. Schedules are drafted with proposed dispositions by the agency Records Officer, and forwarded to and approved by the National Archives and Records Administration.

Records dispositions (i.e., maintain, update, archive, delete or destroy) are required for all AISs, including the system software, documentation, data, output records and backups.

Contact the USPTO Records Officer in the Office of Data Management, Data Administration Division to begin the disposition scheduling process.

The records management (electronic, paper, and other records) requirements for developing automated information systems are contained in the *Life Cycle Management for Automated Information Systems* manual. The Office of Data Management intranet site[4] contains records management (electronic, paper, and other records) policy and procedures documents. Consult the Records Officer for guidance to ensure observance of these records management requirements. For additional information, see the USPTO Comprehensive Records Schedule.

Electronic Records Management

A draft checklist of requirements for electronic records management for an automated information system should be created. Consult the Electronic Records Management Team Leader for guidance and assistance. This checklist will be refined throughout the LCM to reflect more granular business area requirements.

Information Collection Burden

Under the Paperwork Reduction Act (PRA), an agency must gain approval from the Office of Management and Budget (OMB) prior to implementing any program, application, form, or system that involves collecting information, or using information collected from the public. The purpose of the PRA activity is to account for the burden hours the government places on the public and minimizing that burden as much as possible.

An agency also has an obligation to minimize the cost to the Federal Government of obtaining information necessary for the proper performance of Federal agency functions. Estimate any additional information collection burden hours imposed on Federal workers to process the information collected from the public.

The Office of Data Management, Data Administration Division, Records Officer should be consulted for guidelines on the information collection and approval process during the Concept Phase.

[4] Office of Data Management intranet site: http://ptoweb/ptointranet/nodm/odmfrontpage.htm

Table 2.3 is a summary of data management activities for the Concept Phase.

CONCEPT PHASE **Table 2.3**

The Project Manager and System Development Manager works with the Office of Data Management to determine the data management approach, including metadata documentation, electronic and records management requirements, information collection burden, and roles and responsibilities of key players.

DM Tasks	DM Products
Begin data requirements gathering Determine data management approach Identify data stewardship roles and responsibilities Identify data life cycle and tools Determine metadata documentation products Draft Data Management Plan Define high-level data architecture Establish XML Resource repository storing categories Establish preliminary records schedule Identify basic electronic records management checklist requirements Evaluate information collection burden	Draft Data Management Plan High-Level Logical Data or Object Model Draft Electronic Records Management Requirements Checklist

2.4 Detailed Analysis and Design Phase

Activities and plans regarding data management for an AIS project are expanded into more details in this phase. These activities and plans include but not limited to, logical data model; physical data base design; data element standardization worksheets; data stewardship activities; data conversion plan; data quality plan; testing support activities; data back-up, logging, and recovery plans; sensitive data and data base administration activities. Any associated metadata products should be completed before the end of the Detailed Analysis and Design Phase.

2.4.1 Logical Data Model

During the Detailed Analysis and Design Phase, the high-level logical model that was developed in the Concept Phase is refined to a fully attributed model in third normal form. The logical model contains the metadata about logical objects of the system. This includes the object's names, definitions, type, length/precision, domain information (description, range, values), format, etc. The logical model shall use standard data elements, standard abbreviations, and acronyms. Consult the *Data Element Naming Conventions and Standardization Technical Standard and Guideline, IT-212.03-13* for details on naming standards and list of standard abbreviations and acronyms. Developing the logical data model is a joint effort between the Data Administration Division and the AIS system development team. The validated logical data model and the mapping matrix should be completed before the end of the Detailed Analysis and Design Phase.

2.4.2 Physical Data Base Design

As the data model moves from logical design to physical implementation, the entity and attribute names from the logical model are transformed into physical tables and columns in the data base. The *Data Element Naming Conventions & Standardization TSG, IT-212.03-13*, contains a set of rules for naming the physical design data elements: tables, columns, foreign key columns, primary keys, indices, and referential integrity constraints. The naming convention advocated by the USPTO supports use of the common business name, which leads to "end user friendly" and consistent data element names across USPTO AISs. Refer to the *Data Element Naming Conventions & Standardization TSG, IT-212.03-13,* for more information. Consult with Data Administration for assistance and approval of all physical design names.

2.4.3 Data Element Standardization

Standardizing a data element is a required process of a project's data management. Data that are being shared by more than one system or defined as sharable in the *Detailed Design Document* are candidates for standardizing. These candidate data elements should already be defined in the project's logical model. The system developer, with the assistance of the data administrator, is responsible for providing input for the Standard Data Element Worksheet. The Standard Data Element Worksheet can be generated from Enterprise Information Repository. See Appendix E for an example worksheet using Enterprise Information Repository. Refer to the *Data Element*

Naming Conventions and Standardization Technical Standard and Guideline IT-212.03-13, or contact the Data Administration Division staff for further information.

2.4.4 SGML/XML Resources

During the Detailed Analysis and Design Phase the System Development Manager with an assistance from XML Registrar reviews the XML Resource Repository to determine if the XML resources can be used to fulfill the project needs, identifies the XML resources that can be modified to meet the project needs, and determines what new XML resources must be developed. The XML DTDs, schemas, and other XML resources should be incorporated into the project's Detailed Design Document.

2.4.5 Data Conversion

The need for a Data Conversion Plan is defined in the Life Cycle Management documents that are prepared early in the life cycle such as the Concept of Operations, AIS Project Management Plan, and the High Level Technical Architecture. If existing data will be used in the new system, for example, legacy data, Optical Character Recognition, Intelligent Character Recognition, Standard Generalized Markup Language, Hypertext Markup Language, eXtensible Markup Language or electronic imaging technology; include details of plans for data conversion or migration and the support activities.

Detailed information regarding the project's data conversion strategy shall be documented in a separate Data Conversion Plan. See Appendix G for guidance on Data Conversion Plan content. Consult the *Standard Generalized Markup Language (SGML) and eXtensible Markup Language (XML) Resource Management Guidelines Technical Note*[5], *IT-212.2-05: TN01* for details on SGML and XML resource management procedures.

2.4.6 Data Quality

The objective of defining, designing, implementing, and maintaining an AIS is to provide the information needed by an organization for its day-to-day operations and its management decision making. Data must be acceptable to its users if this objective is to be met. Generally, the acceptability of data is judged by two features: its usefulness and its quality. While these data features are well recognized, there are no standard definitions of data usefulness and data quality. This is due largely to the view that these features are subjective in nature and measurable only in a qualitative rather than a quantitative manner. However, data quality can be defined in a manner that permits its quantitative measurement.

Data quality is determined by comparing the data against a standard(s) and measuring the degree to which the data agrees with the standard(s). Data quality is defined by six attributes: accuracy, completeness, consistency, timeliness, uniqueness, and validity. By independently measuring

[5] Consult Office of Data Management for Technical Note: http://ptoweb/ptointranet/nodm/odmfrontpage.htm

the extent to which these six attributes occur and combining them for more in-depth analysis, the overall data quality can be obtained.

Much of the improvement in data quality that an organization requires will occur as a result of following the data management approach carefully. However, data quality should be measured periodically. A Data Quality Management process needs to be established. Instructions for establishing the Data Quality Management process are provided in the *Data Quality Management at the United States Patent and Trademark Office* guideline. Please contact the Office of Data Management for information about this document. The Data Quality Management process should include plans for conducting:

- <u>Baseline Assessment</u> - Overall assessment of the existing data quality condition
- <u>Improvement Monitoring</u> - Track the effect of corrective actions over time by continuously re-testing for critical defects identified in the Baseline Assessment.
- <u>On-going Quality Monitoring</u> - Once the data quality goals for a data environment has been achieved through improvement monitoring and corrective action, the data environment is regularly monitored to ensure that the data quality does not deteriorate.

The establishment of a data quality environment is often ignored. The following additional data quality activities are to be considered: determine data quality environment requirements; determine data quality tools; acquire data quality resources; and establish data quality environment. Data quality is not just a concern for production data bases but it extends to the backup and recovery media. Procedures are to be established for routine validation of backup and recovery media. The system's operational manager should perform routine evaluation of backup media.

2.4.7 Testing Support

Plans to support software program development and unit testing must be considered and recorded. Coordinate the plan carefully to avoid problems. Consult the *Testing Technical Standard and Guideline, IT-212.3-01* for detailed guidance. Identify data base administration support required to support testing activities.

2.4.8 Data Back-up, Logging, and Recovery Plan

Document plans for data back-up, logging, and recovery of the physical data the project creates in the development environment. Identify all data base administration support required to facilitate development activities.

2.4.9 Sensitive Data/Privacy Act Compliance

Many people think that sensitive information only requires protection from unauthorized disclosure. However, the Computer Security Act provides a much broader definition of the term "sensitive" information: "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United

States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."

Briefly identify data security requirements and describe how they will be implemented. Responsibility for identifying sensitive data and protecting the data must be detailed in accordance with the data stewardship roles of the project. Details of data security requirements are recorded by the system development manager in accordance with the *AIS Security Planning TSG, IT-212.2-08* during the Detailed Analysis and Design Task. Document the data sensitivity level on the Data Element Standardization Worksheet.

The Privacy Act establishes certain controls over what personal information is collected by the federal government and how it is used. It applies to records if they are in a "system of records," which means they are retrieved by an individual's name, social security number or some other personal identifier. Notify the Records Officer as to whether or not the system will have Privacy Act implications.

2.4.10 Mapping Matrices

Various metadata products are developed for an AIS project. A mapping matrix is required to document the transformation between metadata products. The following matrices are to be developed when applicable: logical data model attributes to physical data elements; COTS data elements to logical data model attributes; and DTD or schema elements to either the logical data model or to object data in an object-oriented design.

2.4.11 Data Stewardship Implementation Activities

Data stewardship activities continue during the Detailed Analysis and Design Phase. The following data stewardship activities are conducted:

- The data element standardization process can begin as early as the Detailed Analysis and Design Phase. The Project Manager, System Development Manager, and Operational Data Steward work with the Data Administration Division to revise any data element worksheets that do not meet the AIS needs. The revised data element worksheet should be submitted to Data Administration for consideration. Detail information on the data element standardization process is in the *Data Element Naming Conventions and Standardization TSG, IT-212.03-13*. A sample standard data element worksheet can be found in Appendix E of this document.

- The Operational Data Steward will define attributes to describe the data entity types more fully including data type, length, and permitted values. For each attribute, a sensitivity level should be identified. For highly sensitive data elements, the Operational Steward shall identify authorized users who have access to the data element.

- The Project Manager, System Development Manager, and Operational Data Steward will work with the Data Administration Division to continue the data element standardization process by either drafting new standard data element worksheets for new data or submitting revised standard data element worksheets for potential changes to existing standard data elements. For each standard data element, record the Business Area and Operational Data Stewards. Name the organization that will support technical operation of the system and data base once it is in the Operations Phase, and record this organization as the Technical Data Steward for all associated standard data elements. Record the sensitivity level for each standard data element on the standard data element worksheet.

- The Operational Data Steward will define data quality criteria by identifying potential data quality filters.

2.4.12 Data Base Administration Activities

The AIS development team should meet with the Data Base Administration Division to discuss the following topics.

- Data Base Management System (DBMS) products and tools
- Physical data model
- Code reuse
- Data base sizing
- Estimated update volume
- Synchronization
- Shared data
- Data security
- Data Base Administration Division support required to support Development Phase activities, including physical data base creation, data base backup and recovery, data base security controls

2.4.13 Additional Tasks and Responsibilities

Additional data management tasks in the Detailed Analysis and Design Phase include information regarding information collection burden, and records management.

- Information Collection Burden
  The program office should assist in preparing the information burden collection package (as required). Appropriate Federal Register Notice(s), change worksheets and/or a new information collection package should be created Any supporting information, such as a draft of related electronic forms, should be submitted to the Records Officer.

- Records Management
  The Comprehensive Records Schedule will be reviewed to determine if the project will require the development of a new records series or changes to dispositions of existing series.

- Electronic Records Management
  Utilizing the Electronic Records Management Requirements checklist, the SDM and the Operational Records Steward should identify the entity types and data elements that will comprise the vital records for the AIS. Auditable events for use of the records should also be documented.

Table 2.4 shows data management activities for the Detailed Analysis and Design Phase.

DETAILED ANALYSIS AND DESIGN PHASE **Table 2.4**

During this phase, the AIS Development Team and the Data Steward Organization work closely with the Office of Data Management when defining and refining data requirements, developing the detailed logical data model, creating the physical data model, defining the data conversion strategy, the defining data quality approach, defining electronic records management requirements, and planning data base capacity and security controls.

DM Tasks	**DM Products**
Refine detailed logical data model or object model Develop data quality approach Develop data conversion strategy (as required) Create physical data model Begin data element standardization Update Data Management Plan Create mapping matrix Develop/Modify XML resources (as required) Refine records management schedule Identify privacy requirements Begin information burden submission (as required) Refine electronic records management requirements checklist Identify Data Base Administration Division Support requirements for subsequent phase	Updated Data Management Plan Data Quality Plan (as required) Data Conversion Plan (as required) Update logical or object data models Candidate/Revised SDE worksheets Mapping matrix (i.e., logical data model to physical data base, and physical data model to DTD/Schema, AIS physical data elements to physical data elements used in other systems) Records management retention schedule Updated electronic records management requirements checklist Document Data Base Administration Division support requirements

2.5 Development Phase

All data management products and documentation from the Detailed Analysis and Design Phase should be modified as needed in the Development Phase. These activities include completing and validating the physical data model and updating the logical data model with any additional changes, finalizing all associated mapping matrices, refining the electronic records management checklist, continuing data element standardization, analyzing data quality as required, and determining the data quality monitoring schedule.

2.5.1 Data Stewardship Implementation Activities

During the Development Phase the following data stewardship activities are conducted.

- The Operational Data Steward will identify the data elements that are not to be retained for the life of the system. The Electronic Records Keeping System will document the collection period and retention period for each of these data elements. Consult the Electronic Records Management Team Leader for further details.

- The Project Manager and System Development Manager will work with the Data Administration Division to continue the data element standardization process to ensure compliance with the technical design names for the physical data base as defined in the *Data Element Naming Conventions and Standardization TSG IT-212.03-13*.

- The Operational Data Steward will prepare data quality filters, execute baseline assessment, analyze results, and correct data errors.

2.5.2 Metadata Products

In this phase, the logical model is transformed into a physical model. The Data Administration Division will actively participate to ensure that each data element is defined accordingly to the USPTO standard physical naming conventions. In addition, the Data Base Administration Division will assist the developers with physical data definitions to best utilize the Data Base Management System. It is most unusual in this phase for physical data model/definition to change for performance or ease of coding.

If there are changes to the standard data elements that affect the metadata as defined in the worksheet, a revised worksheet for the affected data element will be prepared for approval.

Make provisions for ensuring that all required metadata is provided to the Data Administration Division, Office of Data Management for the agency's Enterprise Information Repository. The data management in this phase should include the activities detailed in the following subsections.

2.5.2.1 Data Models

The development team will complete and validate the logical and physical data models with the business user. The development team will apply the technical design naming standards to the physical data model. The Data Base Administration Division will create the data base schema in the development environment, based on the data base sizing estimate that was completed in the Detailed Analysis and Design Phase. The logical and physical data models will be loaded to the Enterprise Information Repository. Business information from the project's logical and physical data models will be migrated into the Enterprise Data Model.

2.5.2.2 Data Element Standardization

The business user will review the drafted standard element worksheet. The final draft of the standard data element worksheet should be completed before the end of the Development Phase.

2.5.3 Data Quality

The filters for data quality Baseline Assessment and Improvement Monitoring will be developed and executed. The development team and business users will analyze results to ascertain corrective action. The filters to be used to monitor data quality during the Operations Phase will be identified.

2.5.4 SGML/XML Resources

During the Development Phase, XML Resource modification and development activities continue, resulting in the final required DTDs, Schemas, and Style Sheets. XML Resources are to be tested during this phase.

2.5.5 Testing Support

The data source, data base environment requirements, and required Data Base Administration Division support will be identified for unit, integration, and acceptance testing. Consult the *Testing Technical Standard and Guideline, IT-212.3-01* for additional details. The Data Base Administration Division will closely monitor the testing procedures to identify any necessary data base changes needed for the production environment.

2.5.6 Data Base Management Activities

The activities related to the data base administration function include planning for the production data base environment, securing the production version of software, loading production data, plan and schedule implementation activities. These deployment activities should be documented in the *Production Installation Plan*, *Configuration Management Build Instructions*, and *Operational Support Plan*. Consult with the Data Base Administration Division for planning these activities.

2.5.7 Back-up, Recovery, and Restart

The procedures for back-up, recovery, and restart of production data will be defined. The procedures for ensuring that the production environment is recoverable will be documented in the *Operational Support Plan.* Consideration needs to be given to ensure the data quality of back-up data and recovery data.

2.5.8 Records Disposition

Document plans to archive records. Document the AIS records disposition in the *Operational Support Plan.* The data disposition must comply with the *USPTO Comprehensive Records Schedule.* Consult the USPTO Records Officer for further information.

2.5.9 Electronic Records Management

The Electronic Records Management checklist will be revised accordingly. Test for quality, integrity, and security of the records. Document any transition and record conversion requirement in the *Production Installation Plan.* Consult with the Electronic Records Team Leader for additional information.

Table 2.5 shows data management activities for the Development Phase.

DEVELOPMENT PHASE **Table 2.5**

<table>
<tr><td colspan="2">The System Development team works with the Office of Data Management to complete data products, ensuring logical and physical data models adhere to the <i>Data Element Naming Conventions and Standardization</i> guidelines, ensuring XML products adhere to element and resource naming convention, and to establish the data base environment.</td></tr>
<tr><th>DM Tasks</th><th>DM Products</th></tr>
<tr><td>Finalize Data Management Plan
Complete and validate logical and physical models
Apply technical design naming standard to physical model
Continue data element standardization
Finalize XML Resources
Test XML Resources
Perform Data Quality Analysis (as required)
Determine Data Quality Monitoring Approach
Update Electronic Records Management Requirements Checklist
Identify data base environment requirements and Data Base Administration support requirements</td><td>Final Data Management Plan
Final logical and physical model
Revised SDE worksheets
Final XML/Schema Resources
Data Quality Assessment Report (as required)
Updated Electronic Records Management Requirements Checklist
Established data base</td></tr>
</table>

2.6 Deployment Phase

All the data management products from the Development Phase should be modified as needed in the Deployment Phase. The Data Base Administration Division will play an integral part in the Deployment Phase. The Data Base Administration Division will assist developers to ensure that all pieces of the system, from data base configuration and backup to data completeness, are ready for production.

2.6.1 Data Stewardship Implementation Activities

During the Deployment Phase, the Operational Data Steward will determine a schedule for monitoring data quality.

2.6.2 Data Quality

The Data Management Plan should include information regarding the data quality monitoring schedule and error correction process. This includes establishing the frequency for executing the data quality audit of the production data base and establishing error correction process as well as backup media.

2.6.3 Data Base Management Activities

The tasks and responsibilities of the Data Base Administration Division in the Deployment Phase include the following:

- Data Loading
  Work with developer on data conversion and loading.

- Data Base Upgrade
  Plan for future data base software/application upgrades.

- Data Base Monitoring
  Monitor the data base and plan for growth.

- Data Security
  Work with the Office of Information System Security to set up and manage data base user accounts, monitor user accesses to maintain license compliance, and manage file access controls.

- Data Base Tuning
  For optimal performance, tuning should be an on-going process for both the data base configuration and application. The Data Base Administration Division works closely with

the developers and system administrator to make changes as usage, environment and data grow.

2.6.4 Information Collection Burden

Any required information collection submission should be completed. Approved OMB numbers should be applied to any associated forms.

2.6.5 Electronic Records Management

Implement other electronic records management activities per the NARA approved records schedule and as documented in the Electronic Records Management Requirements Checklist. Consult the Electronic Record Management Team Leader for additional information.

Table 2.6 summarizes key data management activities for the Deployment Phase.

DEPLOYMENT PHASE **Table 2.6**

<table>
<tr><td colspan="2">The System Development Manager works with the Office of Data Management to ensure that the data base environment is configured as specified, Enterprise Information Repository updated, and data quality meets business requirements.</td></tr>
<tr><td><b>DM Tasks</b></td><td><b>DM Products</b></td></tr>
<tr><td>Perform Data Quality Monitoring (as required)
Review XML DTD/Schema files
Update Electronic Records Management Requirements Checklist
Submit information collection package for OMB's approval (as required)
Execute data base deployment plan</td><td>Data Quality monitoring report (as required)
Revised Electronic Records Management Requirements Checklist
Approved OMB form number
Deployed production data base</td></tr>
</table>

2.7 Operations Phase

During the Operations Phase modifications are made to a production system to optimize performance and to correct deficiencies. The approach to ensure that all data management operations activities are carried out in support of maintaining the AIS is covered in this section. This section applies to changes made to the AIS after deployment. All other development activities shall adhere to the data management tasks as outlined in the preceding Concept, Detailed Analysis and Design, Development, and Deployment tasks.

The AIS maintenance team and data stewards are to work with the Data Administration staff to maintain the AIS data architecture. This includes the following tasks:

- Logical Data Model - It is the responsibility of the AIS maintenance team to identify and notify the Data Administration Division of new data requirements. The AIS maintenance team shall assist the Data Administration Division in maintaining the logical data model, including revising the AIS logical data model to reflect data architecture changes.

- Physical Data Model - It is the responsibility of the AIS maintenance team to maintain the AIS physical data model. The physical data model shall adhere to all data management policies and guidelines outlined in the *Data Element Naming Conventions and Standardization Technical Standard and Guideline, IT-212.03-13* including all applicable standard data elements and the Enterprise Data Model data structure.

- Standard Data Elements (SDE) - The AIS maintenance team is to ensure that all SDEs are used. The AIS maintenance team is to work with the Data Administration Division to revise SDEs as warranted.

- Data Quality Monitor - The Operational Data Steward(s) shall execute data quality audits and perform error corrections in accordance with the check schedule and error corrections process defined during the Development Phase. This is to be done for both the production data base and the backup media.

- Information Collection Budget - Any changes to the type of collection or the method of collecting information must be brought to the attention of the Records Officer so that appropriate change worksheets and revised submissions can be approved by the Office of Management and Budget.

- Records Management – To ensure proper disposition of agency records there must be a continuing effort to follow the guidance listed for each record series in the USPTO Comprehensive Records Schedule. The Records Officer can assist stewards in this and can provide more information on Records Management responsibilities and methodology.

- Electronic Records Management – Activities supporting Electronic Records Management in the Operations Phase include the transfer of vital records to archival storage on approved long-term storage media and any software or hardware dependant migrations of the records. These are auditable events and should be logged accordingly. The Electronic Records Management Checklist should be used to document other operational events and requirements.

The Data Base Administration Division will provide support to AISs as noted in the Operations Support Plan and related and applicable Service Level Agreements, including identifying performance issues, analyzing event logs, DBMS support, and data base recovery.

Table 2.7 summarizes key data management activities for the Operations Phase.

OPERATIONS PHASE **Table 2.7**

The System Maintenance Manager works with the Data Base Administration Division to tune the data base for optimum performance, manage data base access, ensure data base physical integrity, and to troubleshoot problems. The Business Area and Operational Data Stewards work with the Data Administration Division to ensure data quality is meeting the business information needs.

DM Tasks	DM Products
Maintain all metadata products and documentation (as required) Execute data quality monitoring filters (as required) Fine tune data base performance Follow Records Management Schedule Update Electronic Records Management Requirements Checklist (as required) Update Information Collection Package (as required)	Revised metadata products and documentation (as required) Data Quality Report (as required) Revised Electronic Records Management Requirements Checklist Information Collection Budget report

3 Content and Format

3.1 Documentation Standards

The project's Data Management Plan shall be prepared in accordance with the guidelines described in Appendix B. (See Appendix C for sample template.)

3.2 Evaluation Criteria

Below are listed evaluation criteria for the Data Management Plan to be used during informal and formal reviews.

Completeness and correctness checking:

- Data Management Approach
- Data Stewardship roles and assignments
- Data Quality Management
- Metadata Products: Data models, standard data elements, mapping matrices, and SGML/XML tags, DTD, and Schema
- Records Management
- Information Collection
- Electronic Records Management Requirements Checklist

Consistency checking:

- Data activities are harmonious across phases
- Records management activities are harmonious across phases
- Electronic Records Management activities are harmonious across phases

APPENDIX A
BIBLIOGRAPHY

American National Standard X3.138, Information Resource Dictionary System (IRDS), 1988

Barnett, Arnold, Data Administration and Data Dictionaries, 1990

Bruce, Thomas A., Designing Quality Databases with IDEF1X Information Models, New York, N.Y., Dorset House Publishing, 1992

Data Management Association, Guidelines to Implementing Data Resource Management, DAMA International, Bellevue, WA, 2001

Department Administrative Order 208-3, Major System Acquisitions for the Department of Commerce

Department Administrative Order 212-2, Management of Information Technology

Department Organization Order Series 20-14, Office of Information Resources Management

Departmental Notice 92-16, Departmental Life Cycle Management Policy, September 1, 1992

Departmental Notice 93-3, Establishing Data Administration Programs, March 22, 1993

Departmental Notice 93-4, Data Administration Policy for Department-wide Administrative System, March 22, 1993

English, Larry P., Improving Data Warehouse and Business Information Quality, John Wiley and Sons, Inc., New York, 1999

Federal Information Resources Management Regulation (FIRMR), Part 201-20.103-2 and Part 201-20.203-2

Handbook of Data Management 1998 Edition, Auerbach, 1998

Jacobson, Ivar, Object-Oriented Software Engineering: A Use Case Driven Approach, Addison-Wesley Educational Publishers, Inc., 1996

McFadden, Fred R., Modern Database Management, Addison-Wesley Educational Publishers, Inc., 1999

Martin, James, Business Area Analysis Handbook, James Martin House, England, 1989

Martin, James, Information Engineering: A Trilogy, Englewood Cliffs, N.J.; Prentice-Hall, Inc., 1989

Narayan, Rom, Data Dictionary: Implementation, Use and Maintenance, Englewood Cliffs, N.J.: Prentice-Hall, Inc., 1988

National Archives and Records Administration, A Federal Records Management Glossary, Washington, D.C., 1993

National Archives and Records Administration, Managing Electronic Records: National Archives and Records Administration Instructional Guide Series, Washington, D.C., 1990

National Institute of Standards and Technology (NIST) Special Publication 500-208, Manual for Data Administration, March 1993

Office of Management and Budget Circular A-109, Major System Acquisition

Office of Management and Budget Circular A-130, Management of Federal Information Resources, Appendix IV, Section 8.a (1) and b (2) and (6)

Paperwork Reduction Act of 1980 (Public Law 96-511)

Paperwork Reduction Reauthorization Act of 1986

Paperwork Reduction Act of 1995

Tannenbaum, Adrienne, Implementing A Corporate Repository: The Models Meet Reality, New York, John Wiley and Sons, Inc., 1994

USACE LCM Manager's Guide, Version 2.0, Appendix 8; March 31, 1996

United States Patent and Trademark Office, Office of the Chief Information Officer, Introduction to Life-Cycle Management for Automated Information Systems, Version 01.00.05, November 1994

United States Patent and Trademark Office, Office of the Chief Information Officer, Managed Evolutionary Development Guidebook, June 1993

United States Patent and Trademark Office, Office of the Chief Information Officer, User Interface Specification, Technical Guideline USPTO IT-212.4-10, 16 February, 1995

United States Patent and Trademark Office, Office of the Chief Information Officer, Detail Design Document, Technical Standard and Guideline USPTO IT-212.4-12, March, 2000

United States Patent and Trademark Office, Office of the Chief Information Officer, System Boundary Agreement, Technical Standard and Guideline USPTO IT-212.2-10, February 2001

United States Patent and Trademark Office, Office of the Chief Information Officer, Test Plan, Technical Standard and Guideline USPTO IT-212.3-x01, 19 October, 2001,

United States Patent and Trademark Office, Office of the Chief Information Officer, Data Management Plan Guideline Technical Standard And Guideline, October, 1995

United States Patent and Trademark Office, Office of the Chief Information Officer, Data Element Naming Conventions and Standardization Technical Standard And Guideline, August 2001

United States Patent and Trademark Office, Office of the Chief Information Officer, Data Element Naming Convention and Standardization Technical Standard and Guideline, November 2001

United States Patent and Trademark Office, Office of the Chief Information Officer, Records Management; Comprehensive Records Schedule; January 2001

United States Patent and Trademark Office, Office of the Chief Information Officer, Electronic Records Management Technical Standard And Guideline; November 2001, Draft

United States Patent and Trademark Office, Office of the Chief Information Officer, Total Data Quality Management (TDQM) at the United States Patent and Trademark Office, June 1997

APPENDIX B
DATA MANAGEMENT PLAN
CONTENT DESCRIPTION

DATA MANAGEMENT PLAN CONTENT DESCRIPTION

1. GENERAL

Briefly state the purpose of the system(s) and software to which this document applies.

1.1 Purpose of Document

This paragraph shall briefly describe the purpose of the Data Management Plan.

1.2 Scope (optional)

Briefly state the scope of the system. Consideration should be given in this section for multiple phase projects and when multiple systems are involved.

1.3 Automated Information System Project Type

Explicitly identify the type of Automated Information System (AIS) or infrastructure project. A description of AIS project types can be found in Section 2 of the *Data Management Technical Standard and Guideline, IT-212.02-05.*

1.4 Project References

This section shall list all documents referenced in this specification by number, title, revision, and date.

1.5 Terms and Abbreviations

This paragraph shall list any terms, definitions, or acronyms unique to this document and subject to interpretation by the users of the document.

2. METADATA PRODUCTS

This section describes the various USPTO metadata documentation products. The USPTO metadata documentation products include the following: logical data model, physical data model, standard data elements, SGML/XML products, metadata mapping matrices, records management, electronic records management, information collection burden, data conversion plan, and data quality plan. Section 4 identifies which metadata documentation products are applicable to the project by LCM phases.

3. IDENTIFICATION OF DATA STEWARDSHIP ORGANIZATION

Identify the key players regarding data management activities for the AIS project. At the minimum, the following roles are included: Business Area Data Steward, Operational Data Steward, and Technical Data Steward, along with User(s). Other roles can be added as appropriate and needed.

Prepare a separate *Roles and Responsibilities* appendix listing the names of the individuals performing the above functions.

4. LIFE CYCLE MANAGEMENT PHASES' ACTIVITIES AND PRODUCTS

Identify the data management tasks and the responsible parties for each data management task for each life cycle phase.

4.1 Concept Phase Activities and Products

Describe the data management approach, information collection burden, and records management activities (electronic, paper, and other records) for the project. Define the AIS data management approach, data stewardship, the data management tools, and metadata documentation products.

4.1.1 Data Management Approach

Describe the project's background and information that led to the need to develop the system. Define the project type. Identify the selected data management approach. Define the data management activities by role and function and identify the responsible parties.

4.1.2 Data Management Tools

This section shall identify the automated tools that will be used during the project to support data management activities. If different tools are used, this section shall describe the coordination efforts to keep the tools in sync.

Define plans for managing the flow of metadata through the AIS life cycle. Identify all data management software to be used.

4.1.3 Additional Metadata Products and Activities

Identify metadata products that are required for the AIS project during the Concept Phase. Determine and document plans for developing and maintaining the project's logical data model, metadata, and records management (electronic, paper, and other records).

Identify data management topics to be addressed during the Technical Review Board meeting at the conclusion of the Concept Phase.

All data products and activities must adhere to the requirements described in the *Data Management Technical Standard and Guideline, IT-212.02-05, Data Element Naming Conventions and Standardization Technical Standard and Guideline, IT-212.03-13* and *Standard Generalized Markup Language (SGML) and eXtensible Markup Language (XML) Resource Management Guidelines Technical Note, IT-212.2-05: TN01.*

4.2 Detailed Analysis and Design Phase Products and Activities

Define all data management related activities that will occur in this phase. Emphasize any changes that affect the data management approach and tools as defined in the Concept Phase. Identify the changes that relate to the project's data models and all metadata documentation products such as the Standard Data Element Worksheet, the mapping matrix, data conversion plan, data quality plan, records retention schedule, electronic records management, and Enterprise Information Repository.

Identify data management topics to be addressed during the Technical Review Board meeting at the conclusion of the Detailed Analysis and Design Phase.

4.3 Development Products and Activities

Document physical information for data base. Define the data set or files, physical records, segments, block sizes, data set allocations and physical size limits if possible. Modify the following if there are any changes since the Detailed Analysis and Design Phase.

- Testing Support (Integration and Acceptance Testing)
  - data testing strategy
  - test data acquisition
  - needed resources
- Cutover Plans
- Data Base and Metadata Management
- Data Back-up, Recovery, and Restart
- Records Retention Schedule
- Electronic Records Management
- Data Quality

Identify data management topics to be addressed during the Technical Review Board meeting at the conclusion of the Development Phase.

4.4 Deployment Products and Activities

Define plans to update and maintain the AIS metadata, data base, and Enterprise Information Repository. Determine and record the approach for ensuring all data management evaluation task activities will be carried out in support of operational assessment. This includes data quality monitoring and error correction.

Identify data management topics to be addressed during the Technical Review Board meeting at the conclusion of the Deployment Phase.

Address Deployment Phase topics that were documented during the Concept Phase and update as warranted during subsequent life cycle phases.

4.5 Operations Products and Activities

The approaches to ensure that all data management activities are performed in support of the AIS maintenance are covered in this section. This section applies to changes to AISs after deployment. The following metadata products and activities are required for the Operations Phase of the LCM: maintain metadata products, maintain electronic records audit trail, maintain data base and backup media data quality, maintain records disposition schedule, and monitor data base performance.

APPENDICES

Appendices shall be used as cited above in Section 3 and may be used to provide information published separately for convenience in document maintenance. As applicable, each appendix shall be referenced in the main body of the document where the data would normally have been provided. Appendices shall be lettered alphabetically (A, B, etc.).

Attachment 9

APPENDIX C
DATA MANAGEMENT PLAN TEMPLATE

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES PATENT AND TRADEMARK OFFICE

Data Management Plan

for the

[*Insert Project Name*]

[Insert Date]

Prepared by:
OFFICE OF DATA MANAGEMENT
DATA ADMINISTRATION DIVISION

Approved By:

Project Manager	System Development Manager	Director, Office of Data Management

DATA MANAGEMENT
TABLE OF CONTENTS

1. GENERAL

Briefly state the purpose of the system(s) and software to which this document applies.

1.1 Purpose of Document

The purpose of the Data Management Plan for the [***insert specific project name***] project is to outline the specific data management, information collection burden, and records management (electronic, paper, and other records) activities that apply to the development and maintenance of [***insert specific project name***]. The plan identifies responsibilities for performing the tasks and when they are to be completed. The Data Management Plan (DMP) addresses specific tasks for the following life cycle phases: (1) Concept; (2) Detailed Analysis and Design; (3) Development; (4) Deployment; and (5) Operations. This document will review data management related activities to date and discuss in detail data management activities for the [***insert specific project name***] project from the Concept Phase through the Operations Phase. The DMP is an evolutionary document and is updated as needed during each life cycle phase.

1.2 Scope

Briefly state the scope of the system(s) involved in this project. The [***insert specific project name***] project requires modifications to multiple AISs. This DMP covers all AISs required to make changes for the [***insert specific project name***]. All AISs making changes to accommodate the [***insert specific project name***] shall adhere to the data management practices documented in this DMP.

1.3 Automated Information System Characteristics

The [***insert specific project name***] is:
(check all that apply)

______ Commercial-Off-The-Self Application Project
______ Government-Off-The-Self Application Project
______ Integrated-Computer Aided Software Engineering Based Project
______ Object-Oriented Based Project
______ Multiple Phased Project
______ Mixed Solution
______ Multiple, Related Automated Information Systems
______ Component Based Project

A description of the various AIS metadata products can be found in Section 2. The specific metadata products required for this Automated Information System (AIS) is outlined in Section 4.

1.4 Project References

The following documents were used as a basis for development of the [*insert specific project name*] DMP:

[List documents]

1.5 Terms and Abbreviations

This section list terms, definitions, or acronyms unique to this document and subject to interpretation by the users of the document.

[*List unique terms and abbreviations*]

2. METADATA PRODUCTS

Metadata is the foundation for establishing a common enterprise data architect. Data documentation is an important and indispensable part of the USPTO common data architecture. The USPTO metadata documentation products include the following: logical data model, physical data model, standard data elements, SGML/XML products, metadata mapping matrices, records management, electronic records management, information collection burden, data conversion, and data quality. This section describes the various USPTO metadata documentation products. Section 4 identifies which metadata documentation products are applicable to the [***insert specific project name***] by LCM phases. All metadata products are to be loaded into the Enterprise Information Repository.

2.1 Logical Data Model

Data modeling is the activity through which data requirements are identified and the data requirements are structured into logical data models. The objective of this task is to describe the things of interest to the business within the scope of the AIS, the relationships between them, and the business rules imposed by the program office. The logical model is developed by the Office of Data Management, Data Administration Division and is validated by the System Development Manager and business users. Depending upon the methodology used, the logical data model can be expressed in different forms. When information-engineering approach is used, the logical data model is expressed in the form of an Entity Relationship Diagram. When Object-Oriented approach is used, the logical data model is expressed in the form of a Class Diagram.

2.1.1 Entity Relationship Diagram

The entity relationship diagram (ERD) is a pictorial representation of the data needs. The ERD is a logical data model that contains entities, attributes, and relationships. All ERDs are normalized to third normal form.

2.1.2 Class Diagram

The class diagram shows the static structure of an object-oriented model: the object classes, their internal structure, and the relationships in which they participate. The class diagram should include the class name, list of attributes, list of operations, and class associations.

2.2 Physical Data Model

The physical data model is a data model adapted to meet the constraints of a specific Data Base Management System. It is a modification of the logical data model that can be tuned for performance or security purposes.

2.3 Standard Data Elements

Standardization of data elements is key to the development of an enterprise-wide data architecture. A common data architecture addresses data problems, such as inaccuracy, inconsistency, data maintenance expenses, and lack of data integration. Standardization requires that all existing and new data be defined in a common context so that the data can be easily understood and readily shared. Each element needs to be understood in terms of what it means, then it needs to be uniquely identified, defined, named, and related appropriately. All logical and physical data elements shall conform to the USPTO data element naming conventions and standardization policies as documented in the *Data Element Naming Conventions and Standardization Technical Standard and Guideline, IT-212.03-13.*

2.4 SGML/XML Products

When Standard Generalized Markup Language/eXtensible Markup Language (SGML/XML) products are created, the following metadata products shall be generated: Document Type Definition (DTD), Style Sheet, document instances, and templates. Information contained in these documents should be linked to the AIS's logical data model, especially the DTD tags. This activity demonstrates a mapping between the data elements of the logical data model and the tags in the DTDs. XML DTDs, schemas, and other XML resources are to be included in the AIS' Detail Design Document. All versions of DTDs, Schemas, Style Sheets, samples of Document Instances, Public Entities, definitions of USPTO-established XML Namespaces, Templates, and associated documentation shall be stored in the XML Resource Repository. Consult the *Standard Generalized Markup Language (SGML) and eXtensible Markup Language (XML) Resource Management Guidelines Technical Note, IT-212.2-05: TN01* and the *Detail Design Document* Technical Standard and Guideline for specific details and examples.

2.5 Metadata Mapping Matrices

During the project life cycle, multiple metadata products are produced. A mapping matrix is required to document the transformation between metadata products. The mapping matrices include:

- between the logical data model attributes and physical data elements;
- between COTS data elements and logical data model attributes; and
- between elements in a DTD or schema to either the logical data model or to object data in an object-oriented design.

For examples see the *Standard Generalized Markup Language (SGML) and eXtensible Markup Language (XML) Resource Management Guidelines Technical Note, IT-212.2-05: TN01* and Appendix F of the *Data Management Technical Standard and Guideline, IT-212.2-05.*

2.6 Records Management

Records Management is an USPTO-wide activity. An active, effective USPTO-wide Records Management program is required by law. Such a program supports ongoing operations efficiently and facilitates the reengineering of USPTO business processes. A well-executed vital records program supports disaster recovery. The [***insert specific project name***] project must adhere to the record disposition schedule for each AIS as outlined in the *United States Patent and Trademark Comprehensive Records Schedule* and the *Records Management Handbook.*

2.7 Electronic Records Management

Attention to electronic records management is crucial to successful information technology planning and must go hand-in-hand with development of automated information systems. Electronic records shall be tracked in a record keeping system from creation. The record keeping system used must be approved in accordance with the USPTO Technical Reference Model. For specific details consult the Electronic Records Management Team Leader for guidance.

2.8 Information Collection Burden

Under the Paperwork Reduction Act, the United States Patent and Trademark Office has an obligation to minimize the cost to the Federal Government and minimizing the burden that government places on the public of obtaining information necessary for proper performance of Federal agency functions. This information collection burden extends beyond paper collection to electronic collection.

If it is anticipated that information is to be collected from a non-USPTO source, the program office is to review information collection mediums to determine if they meet the AIS needs. When new data is to be collected, it is recommended that standard data element names and data structure be considered. Using standard data elements allows uniformity for the data life cycle and supports consistency throughout the enterprise;thus reducing the ambiguity of the data element among USPTO business areas. If a standard data element does not exist, please refer to the *Data Element Naming Conventions and Standardization Technical Standard and Guideline, IT-212.03-13* for naming new data elements. The business user should work with the Office of Data Management to prepare the appropriate Information Collection Burden package for the Office of Management and Budget approval.

2.9 Data Conversion Strategy

If existing data will be used in the new system, for example, legacy data, Optical Character Recognition, Intelligent Character Recognition, Standard Generalized Markup Language, Hypertext Markup Language, eXtensible Markup Language or electronic imaging technology, include details of plans for data conversion or migration and the support activities. Consult Appendix G of the *Data Management* Technical Standard and Guideline for additional guidance.

2.10 Data Quality Assurance

The value of automated information systems is dependent upon the quality of the information they provide. However, the quality of AIS information is only as good as the data from which it is derived. With the advent of the Internet, we can no longer minimize the importance of the quality of the enterprise's data. Therefore, it is imperative that attention be given to data quality. The approach for addressing data quality should be an integral part of the AIS development, especially for data conversion and data migration projects. The approach should include data quality measuring, reporting, error correction, and on-going data quality monitoring and error correction procedures. The approach should extend beyond the operational system to the backup and recovery data. For guidance see *Total Data Quality Management (TDQM) at the United States Patent and Trademark Office* on the Office of Data Management website (http://ptoweb/ptointranet/nodm/dmg.htm).

3. IDENTIFICATION OF DATA STEWARDSHIP ORGANIZATION

Data stewardship encompasses the functions and responsibilities of an organization that exercises programmatic control over data on behalf of the program. The Data Stewardship organization is responsible for determining and documenting the data the system will collect and process. The data stewardship functional roles that must be performed for system development and maintenance are: Business Area Data Steward, Operational Data Steward, and Technical Data Steward, along with User(s). The following section provides descriptions of the data stewardship roles and Appendix A, Roles and Responsibilities, identifies the USPTO staff filling these roles for the [***insert specific project name***] project.

3.1 Business Data Steward

The Business Area Data Steward has overall responsibility for a business area's performance and is responsible for ensuring that the quality of data required to support the business area is defined, collected, processed, stored, and presented in a timely and cost-effective manner. The Business Data Steward role, during a system development effort, includes the Program Sponsor and the Project Manager.

3.1.1 Program Sponsor

The Program Sponsor is responsible for overall project management. The Program Sponsor makes resources available to support the AIS or infrastructure system, defines and validates customer requirements, and reviews progress at each LCM milestone. The Program Sponsor defines the data and functional requirements. The Program Sponsor appoints the Project Manager.

3.1.2 Project Manager

The Project Manager is responsible for overseeing the complete effort to implement the AIS or infrastructure system. The Project Manager provides daily direction, coordination, and control for all aspects of the design, development, and deployment of the AIS or infrastructure system under the technical direction of the Office of the Chief Information Officer (CIO) and the business direction of the Program Sponsor. Utilizing matrix management, the Project Manager directs the day-to-day activities of all members of the project team. The Project Manager must ensure that all tasks and functional roles for data management planning are performed adequately in order to provide an AIS or infrastructure system of sufficient quality to support program missions.

3.2 Operational Data Steward

The Operational Data Steward is the subject matter expert from the organization or function who is responsible for the definition and collection of data. Since the level to which an organization understands its data directly correlates to the level of success of any AIS, it is the role of the Operational Data Steward to define the metadata or characteristics about the data used in their business functions, along with the derivation rules and the formats to be used for data derived from other data elements. When multiple functions or organizations use the same data to support important program functions, a joint data definition effort is organized.

3.3 Technical Data Steward

The Technical Data Steward comes from the organization responsible for the storage and processing of data in the AIS. The functions carried out by the Technical Data Steward include those that have traditionally been performed by Automated Data Processing (ADP) organizations, such as the System Development and Maintenance Managers, Data Base Administrators, and Data Maintenance Branch/Operations staff. The Technical Data Steward has direct control of the data, software, and hardware components used to:

- Store, process, communicate, and present data;
- Ensure physical integrity of the data;
- Safeguard the storage media;
- Act as Records Management contact; and
- Acts as Paperwork Reduction Act contact.

Since both the Operational and Technical Data Stewards are responsible for ensuring that the data administration standards are met when defining and documenting data, the stewards will rely on the procedures contained in the *Data Element Naming Conventions and Standardization Technical Standard and Guideline, IT-212.03-13* when defining data. The Enterprise Information Repository should also be reviewed for already existing standard definitions of data.

During the development life cycle, this stewardship role will be assigned to the System Development Manager until the system is turned over to the operating organization at which time the stewardship role transfers to the Maintenance Manager, Data Base Administrators, and/or Data Maintenance Branch/Operations staff.

3.3.1 System Development Manager

The SDM, appointed by the CIO, is responsible for the design, development, and deployment of the AIS or infrastructure system under the direction of the Project Manager. The SDM ensures that the system is consistent with the agency's strategic information technology plans.

3.3.2 System Maintenance Manager, Data Base Administrators, and/or Computer Operations staff

The Maintenance Manager, Data Base Administrators, and/or the Computer Operations staff are responsible for the operation of the AIS or infrastructure system. The Maintenance Manager is responsible for the day-to-day operations of the system and for ensuring that the operational system remains consistent with the agency's strategic information technology plans.

The Data Base Administrators are responsible for ensuring that the data is available for operations as outlined in the Operational Support Plan.

The Computer Operations staff is responsible for ensuring that the infrastructure required to support the system is available in accordance with the requirements described in the Operational Support Plan.

3.3.3 User(s)

The organization(s) that use the system are documented in the DMP. The users of a system are categorized into two groups: Primary Users and Ancillary Users.

3.3.4 Primary User

The Primary User collects, stores, and processes the AIS or infrastructure system data. In addition, the Primary User supports user testing during the LCM Deployment phase.

3.3.5 Ancillary User(s)

These users require data used to perform business area functions, and report results to management, Congress and others outside the agency. The ancillary users must rely upon others to define and allow them access to the data.

4. LIFE CYCLE MANAGEMENT PHASES' ACTIVITIES AND PRODUCTS

This section identifies the data management tasks and the responsible parties for the data management activities for each life cycle phase.

4.1 Concept Phase Activities and Products

This section describes the data management, information collection burden, and records management (electronic, paper, and other records) for the [***insert specific project name***] project. It defines the AIS data management approach, data management tools, and identifies the required metadata documentation products.

4.1.1 Data Management Approach

The data management approach has a major influence on the success of a large automation project. The data related activities, products, and decisions that must be addressed during the system life cycle constitute the data management approach. The approach also includes the degree of rigor to be followed when performing these activities and the level of formality to be used when documenting data-related life cycle products and decisions.

A major element for determining the data management approach is the project scope. Several factors are used to determine the project scope. They include: data sharing, and project type. [***insert details regarding the specific project data management approach selection***]

The following table provides a summary of tasks by function and responsible organization for the data management planning process.

Summary of Data Management Activities by Roles

FUNCTION ⇒ ROLE⇓	Data Planning	Prepare and Review Data Management Plan
Program\Project Management	Consult with Data Administration on the data management approach and support the identification of data stewardship and data quality	Review and assist as needed in the development of the Data Management Plan.

FUNCTION ⇒ ROLE⇓	Data Planning	Prepare and Review Data Management Plan
System Development Management	Provide support for data management development activities Coordinate data management activities for compliance with Data Management Plan Comply with Data Management Plan	Review and submit Data Management Plan for review to Quality Assurance, Program Management, Configuration Management, System Architecture and Engineering, Operations, Testing, and End-Users
Office of Data Management	Provide support in using the Enterprise Information Repository	Conduct impact analyses, train, and generate special reports
Data Administration	Prepare Data Management Plan Evaluate and select data approach, methodology, and tools Provides data administration expertise for the preparation of Data Management Plan Provides XML expertise for the preparation of XML DTD/Schema development Evaluate data resources and acquisition, data quality management, records management (electronic, paper, and other), and information collection burden Provide support for the development of the logical data model Provide support for the physical data model ensuring adherence to data element naming convention and enforcement of referential integrity Provide support for standardization of data element	Prepare, Update, and Submit Data Management Plan to System Development Manager Evaluate and approve Data Management Plan for compliance with data administration policies and procedures Evaluate and approve XML DTD/Schema for compliance with SGML/XML Resources Management Guidelines
Data Base Administration	Provide data base administration expertise in planning for development and maintenance of physical data base, including operational impact analysis, data model analysis, implementation impact analyses Plan and schedule development and operational data base implementation, and coordinate with SDM and OSAE regarding data capacity Advise on DBMS and support tools	Evaluate compliance to technical standards for physical maintenance of data resources

FUNCTION ⇒ ROLE ⇓	Data Planning	Prepare and Review Data Management Plan
System Architecture and Engineering	N/A	Review Data Management Plan for compliance with Technical Reference Model and Information Technology infrastructure
Quality Assurance (QA)	Evaluate Data Management Plan for compliance with LCM	Review Data Management Plan
Configuration Management (CM)	N/A	Place Data Management Plan under CM
Operations	Provide support for data management deployment activities	Review Data Management Plan
End-User Involvement	Participate in data stewardship assignments, data resources, and acquisition Perform data quality monitoring	Review Data Management Plan

4.1.2 Data Management Tools

The number and type of data management tools will depend upon the scope of the AIS. Data management tools are generally categorized into four groups: analysis tools, development tools, implementation tools, and delivery tools.

The [*Insert specific project name*] project shall use the following data management tools:
_________ COOL:Gen
_________ Rochade
_________ XML Cannon Repository Tool Suite
_________ Quality Manager
_________ *df*Power
_________ Rational Rose UML Tool
_________ Versatile
_________ DBMS (*supply name*)
_________ Other (*supply name*)

4.1.3 Additional Metadata Products and Activities

The following metadata products and activities are required for the Concept Phase of the LCM for the [*Insert specific project name*] project:

_________ Develop High Level Logical Data Model from Enterprise Data Model
_________ Determine Information Collection Burden Requirement
_________ Establish Preliminary Records Schedule
_________ Identify Basic Electronic Records Management Requirements
_________ Establish categories for storing resources in XML Resource Repository

During the Technical Review Board (TRB)'s review, the following data management topic(s) should be addressed (when applicable):

- Approved DMP
- Re-Use Opportunities (components and data sharing)

All data products and activities must adhere to the requirements outlined in Section 2 where applicable and the *Data Management* Technical Standard and Guideline.

4.2 Detailed Analysis and Design Phase Products and Activities

The following metadata products and activities are required for the Detailed Analysis and Design Phase of the LCM of the [*Insert specific project name*] project:

_________ Develop Detailed Logical Data Model
_________ Develop Detailed Physical Data Model
_________ Identify which XML resources in the XML Resource Repository can be used
_________ Develop/Modify XML resources
_________ Identify Database Management System (DBMS)
_________ Identify shared data opportunities
_________ Create/Modify Standard Data Element Worksheet
_________ Prepare Metadata Mapping Document(s)
_____ Logical data model attributes to physical data elements
_____ COTS data elements to logical data model attributes
_____ DTD or schema elements to logical data model attributes
_____ DTD or schema elements to object data in an object-oriented design
_________ Prepare Information Collection Burden (ICB) OMB package
_________ Revise/Update Records Schedule
_________ Update or develop Electronic Records Management Requirements
_________ Address Vital Records and Privacy Act requirements
_________ Develop Data Conversion Strategy
_________ Develop Data Quality Approach

During the Technical Review Board (TRB)'s review, the following data management topic(s) should be addressed (when applicable):

- Current DMP
- Validated Logical data model
- Data base scheme finalized
- XML resources established
- Metadata mapping documents completed
- ICB package status
- Records Schedule established
- Electronic Records Management Requirements identified
- System data and records retirement plans
- Re-Use Opportunities (components and data sharing)
- Number of Standard Data Element(s) (SDEs) used
- Data Conversion Plan completed
- Data Quality Approach finalized

All data products and activities must adhere to the requirements outlined in Section 2 where applicable and the *Data Management* Technical Standard and Guideline.

4.3 Development Products and Activities

The following metadata products and activities are required for the Development Phase of the LCM of the [***Insert specific project name***] project:

_________ Finalize Database Schema
_________ Finalize Standard Data Element Worksheet
_________ Finalize Metadata Mapping Document(s)
_________ Finalize Records Schedule
_________ Implement Electronic Records Management System
_________ Update Information Collection Burden OMB package
_________ Produce Data Definition Language (DDL)
_________ Test XML resources
_________ Establish Development Database
_________ Establish Test Database
_________ Implement Data Conversion Strategy
_________ Establish Data Quality Audit environment
_________ Conduct Data Quality Audit
_________ Perform Data Error Correction

During the Technical Review Board (TRB)'s review, the following data management topic(s) should be addressed (when applicable):

- Current DMP
- Metadata products finalized
- Metadata mapping documents completed
- XML Resource Test Report
- ICB package status
- Data Quality Audit Report
- Data Error Correction Report
- Records Schedule finalized
- Electronic Records Management System implemented
- System data and records retirement plans status
- Re-Use Opportunities (components and data sharing)
- Number of Standard Data Element(s) (SDEs) used
- Data Conversion status
- Data Quality Approach finalized

All data products and activities must adhere to the requirements outlined in Section 2 where applicable and the *Data Management* Technical Standard and Guideline.

4.4 Deployment Products and Activities

The following metadata products and activities are required for the Deployment Phase of the LCM of the [***Insert specific project name***] project:

_________ Update Enterprise Information Repository
_________ Update XML Resource Repository
_________ Established Production Database
_________ Determine Data Quality Monitoring Schedule
_________ Determine Backup Media Data Quality Approach

During the Technical Review Board (TRB)'s review, the following data management topic(s) should be addressed (when applicable):

- Enterprise Information Repository updated
- XML resources repository updated
- Data Conversion Completed
- Production Database established

All data products and activities must adhere to the requirements outlined in Section 2 where applicable and the *Data Management* Technical Standard and Guideline.

4.5 Operations Products and Activities

The following metadata products and activities are required for the Operations Phase of the LCM of the [***Insert specific project name***] project:

_________ Maintain Metadata products
_________ Maintain Electronic Records Audit Trail
_________ Perform Data Quality Monitoring and Data Error Correction of Production Database
_________ Perform Data Quality Audit of Backup Media
_________ Data Base performance tuning
_________ Adhere to Records Disposition Schedule(s)

All data products and activities must adhere to the requirements outlined in Section 2 where applicable and the *Data Management* Technical Standard and Guideline.

APPENDIX A
ROLES AND RESPONSIBILITIES

ROLES AND RESPONSIBILITIES

BUSINESS DATA STEWARD

Program Sponsor:	[***insert program sponsor's name, title***] [***insert program sponsor's office name***]
Project Manager:	[***insert project manager's name, office name***]

OPERATIONAL DATA STEWARD

[***insert specific project name***] Administrator (s) [***insert operational data steward's name, office***]

TECHNICAL DATA STEWARD

System Development	[***insert technical data steward's name, office***]
System Maintenance Manager	TBD
Data Base Administrator	
Primary	[***insert primary dba's name***], Office of Data Management, Data Base Administration Division
Secondary	[***insert secondaryy dba's name***], Office of Data Management, Data Base Administration Division
Computer Operations Staff	Office of System and Network Management, Central Computer Operation Branch

USERS

Primary User(s):	[***insert the office name of the primary user(s)***]
Ancillary User(s):	[***insert the office name of the ancillary user(s) or N/A for not applicable***]

ADDITIONAL RESPONSIBILITIES

Model Manager(s):	
Logical	[***insert Data Administrator's name***], Office of Data Management, Data Administration Division
Physical	[***insert Data Base Administrator's name***], Office of Data Management, Data Base Administration Division
Records Coordinator	[***insert Records Coordinator's name, office name***]
Records Officer	Susan Brown, Office of Data Management, Data Administration Division

APPENDIX D
GLOSSARY

GLOSSARY

Ancillary User(s): Organization or individual that use data to perform mission functions, and reports results to management, the Congress, and to others outside the agency.

Archives (records management/all media usage): (1) The non-current records of an organization, preserved because of their continuing or enduring value. "National Archives of the United States" means those records that have been determined by the Archivist of the United States to have sufficient historical or other value to warrant their continued preservation by the Federal Government and that have been transferred to the Archivist's legal custody and (2) the organization or agency responsible for appraising, accessioning, preserving, and making available permanent records. In the U.S. Government, the National Archives and Records Administration (NARA).

Archiving (Automated Data Processing usage): In electronic records, the process of creating a back-up copy of computer files, especially for long-term storage, backing up making a copy of a computer file for use if the original is lost, damaged, or destroyed.

Behavior: Represents how an object acts and reacts.

Collection of Information: A request for answers to identical questions, and/or for the compilation and maintenance of records.

Data: Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or automated means.

Data Administration. A high-level function that is responsible for the overall management of data resources in an organization, including maintaining enterprise-wide definitions and standards.

Data Base Management System: A software application that is used to create, maintain, and provide controlled access to user data bases.

Data Definition Language: Those commands used to define a data base, including creating, altering, and dropping tables and establishing constraints.

Data Integrity: The condition in which data is current, consistent, and accurate.

Data Steward: Organization or individual designated from within business areas to safeguard and share data. Business areas that exercise programmatic control over data have data stewardship responsibilities. As a business expert, the data steward identifies and defines data from a business perspective, participates in aspects of data administration, and facilitates data sharing outside the steward's organization. Stewards supply descriptions, definitions, and domain and security requirements for their subject data.

Data Stewardship: Functions and responsibilities of an organization that exercise programmatic control over data on behalf of the program.

Data Validation: Checking data for correctness and compliance with applicable standards, rules, and conventions.

Electronic Records: electronic, or machine-readable records, are records on electronic media. Electronic record, as defined in NARA regulations (36 CFR 1234.2), means any information that is recorded in a format that only a computer can process and that satisfies the definition of a Federal record per the Federal Records Act.

Electronic Records Management: techniques to manage automated records regardless of its format. Electronic Records Management is the broadest term that refers to electronically managing records on varied formats.

Information Collection Burden: Time, effort, or financial resources required to respond to a collection of information.

Information Repository: A knowledge base that integrates an enterprise's business information and application portfolio.

Logical Data Model: A representation of the organization's business data at its logical level including all principal subject areas, entity types, relationships and attributes of interest to the business, while maintaining technological neutrality.

Metadata: Data describing data, such as definition, source, responsible organization, format, and range of values. Metadata is organized in the form of entities, attributes, and relationships, and is generally stored in an enterprise information repository.

Object: An entity that has a well-defined role in the application domain, and has state, behavior, and identity.

Physical Data Model: A representation of the data base scheme, including detailed structure of the data and how it will be stored. Names and attributes should be enforced/carried over from the logical model.

Primary User(s): Organization or function with the most important requirement to collect, store, and process data to perform a current or future mission function.

Repository: A software tool for management of data and information that provides a mechanism for storing and processing descriptions of information and data processing resources.

State: Encompasses an object's properties (attributes and relationships) and values those properties have, and its behavior. An object's state is determined by its attribute values and links to other objects.

APPENDIX E

STANDARD DATA ELEMENT WORK SHEET

STANDARD DATA ELEMENT WORK SHEET

COUNTRY Code		
1.	Submitter's Name:	Kathryn Tindle
2.	Submission Date:	July 20, 2000
3.	Phone Number:	703-308-7395
4.	Office:	Office of Data Management, Data Administration Division
5.	Automated Information System(s):	Enterprise Address Data Component Application Capture and Review System PALM MG Pre-Exam Patent Application Capture and Entry PCT Operations Workflow and Electronic Review Revenue Accounting Management System Electronic Application Compliant System
6.	Common Business Name:	Country Code
7.	Candidate Data Element Name:	COUNTRY Code
8.	Data Element Description:	The code that represents the officially designated abbreviation for a country according to the International Organization for Standardization (ISO) under International Standard 3166-1.
9.	Data Element Disposition:	Standard
10.	Type:	Alphabetic
11.	Length/Precision:	CHAR 2
12.	Format:	N/A
13.	Alias(es):	N/A
14.	Domain Description:	N/A
15.	Domain Range:	N/A
16.	Domain Values:	Please refer to the International Standard 3166-1 from the International Organization for Standardization (ISO). These approved codes for use at USPTO are stored in the PTO STND COUNTRY group based on the PTO STND ISO 3166-1 table. Note: The World Intellectual Property Organization works closely with ISO so the WIPO country codes are the same as the ISO codes for countries.
17.	SGML/XML Tag:	CTRY, B130
18.	Standard Abbreviated Programming Name:	N/A

19.	Existing Programming Name(s):	CTRY_CD COUNTRY_CODE
20.	Authority:	ISO 3166-1 WIPO ST.3
21.	Sensitivity Level:	Low
22.	Data Structure Reference:	N/A
23.	Unit of Measure:	N/A
24.	Integrity Rules:	Since WIPO ST.3 includes both country codes and international patent organization abbreviations, only the country codes portion of the list are allowed into this address domain.
25.	Model Reference(s):	1) EADC_R01_V02_DANL_A_X of COOLCSE1 2) ICT2_R02_V03_CMPI_A_O of COOLCSE1 3) ICT2_R02_V03_CMPS_A_O of COOLCSE1 4) IEA1_R01_V06_CMPS_A_O of COOLCSE1 5) IEA1_R01_V07_CMPI_A_O of COOLCSE1
26.	Other Source:	APS Green Book Page 3 EFID Dictionary Field 3.32c, Page 151 Field 3.33e, Page 158 Issued Patents Data Dictionary Page A-34 PALM Data Dictionary Page 420 USPAT Reload Data Base Specification Page D-41
27.	Mission Area Reference:	Dissemination, Patents, Trademarks
28.	Business Area Reference:	Dissemination, Patents, Trademarks
29.	Business Data Steward:	Name: Robert Saifer Title: Director, International Liaison Staff Phone: Crystal Park Three, Suite 902 Address: 703-308-6853
30.	Operational Data Steward:	Name: Ed Rishell Title: International Liaison Staff Phone: 308-6867 Address: Crystal Park Three, Suite 902
31.	Technical Data Steward:	Name: Phong Ly Title: Manager, System Development Infrastructure Phone: 305-8719 Address: Crystal Park Three, Suite 402

APPENDIX F

SAMPLE MAPPING MATRIX

SAMPLE MAPPING MATRIX

Existing TRAM System						TRAM Replacement System			
Data Set Name	Volumes	Item Name	Business Name	Length	Type	Disposition	Entity Type	Attribute	Notes
Application Mark	2,197,152	AM-ADDR.PTODB1	Correspondence Address (occurs 5)	40	ALPHA	Modeled	Address	All Address attributes; when Functional Role Type = Correspondent	
		AM-ATTY-DKT-NUM.PTODB1	Attorney Docket Number	12	ALPHA	Modeled	Application SubType	Attorney Docket Number	
		AM-BTCH-NUM.PTODB1	Batch Number	3	ALPHA	Not Modeled: The decision on whether to process case files in batches and what data is needed to support it will be made during design.			
		AM-CHRG-TO-LOC.PTODB1	Charge to Location	3	ALPHA	Modeled: Through relationship between Case File and Case File Location			TBD: through "charge to" relationship to location?
		AM-CHRG-TO.PTODB1	Charge to Employee	5	NUMBER	Modeled: Through relationship between Case File and Employee			TBD: through "charge to" relationship to functional association?
		AM-CLS-CT-ACTV.PTODB1	Class Count - Active	2	NUMBER	Not Modeled: The count of active classes can be derived through Goods and Services entity type or can be added as a design attribute if performance warrants			

AM-CNCL-CD.PTODB1	Cancellation Code	1	ALPHA	Modeled	Registration SubType	Cancellation Code	Stored as 1 character vs. 5 character because first 4 characters are always "CNCD"

APPENDIX G
DATA CONVERSION PLAN
TABLE OF CONTENTS

DATA CONVERSION PLAN

TABLE OF CONTENTS

Attachment 10

OVERVIEW OF LIFE CYCLE MANAGEMENT

1.1 Introduction

1.1.1 Purpose

This Life Cycle Management Manual establishes management policies, procedures, and practices governing the initiation, definition, design, development, deployment, operation, maintenance, enhancement, and retirement of automated information systems[1] (AIS) at the United States Patent and Trademark Office (USPTO).

1.1.2 Objectives

Life Cycle Management (LCM) emphasizes decision processes that influence system cost and usefulness efficiencies. These decisions must be based on full consideration of business functional requirements and economic and technical feasibility in order to produce an effective system. The objectives of the LCM approach are to:

The primary objective of life cycle management is to deliver quality systems when promised and within cost estimates using an identifiable, measurable, and repeatable process.

- deliver quality systems which meet or exceed customer expectations when promised and within cost estimates.
- deliver systems that work effectively and efficiently within the current and planned information technology infrastructure.
- deliver systems that are cost-effective to enhance and maintain.
- develop quality systems using an identifiable, measurable, and repeatable processes.
- establish an organizational and project management structure with appropriate levels of authority to ensure that each AIS or infrastructure project is effectively managed throughout its life cycle.

[1] An automated information system (AIS) is a combination of functional users, information technology personnel, business processes and procedures, application software, system software, documentation, commercial off-the-shelf software, computer, networking and other information technology resources that collect, record, process, store, communicate, retrieve, display, and disseminate information.

- Identify and assign the roles and responsibilities of all affected parties including functional and technical managers throughout the AIS or infrastructure system life cycle.
- Ensure that AIS or infrastructure system requirements are well defined and subsequently satisfied.
- Provide visibility and comprehensive information to USPTO functional and technical managers for all AIS or infrastructure system resource requirements and expenditures.
- Establish appropriate levels of management authority to provide timely direction, coordination, control, review, and approval of the AIS or infrastructure system project.
- Ensure project management accountability.
- Identify project risks early and manage them before they become problems.

1.2 Intended Audience

The primary audience for this Manual and the supporting Technical Standards and Guidelines (TSGs) are the functional and technical managers responsible for defining and delivering USPTO systems, their staff and their support contractors.

1.3 Types of Projects

AIS or infrastructure system projects vary in scope and diversity from simple to complex. Examples of USPTO project types include:

AIS or infrastructure system projects vary in scope and diversity from simple to complex, from the installation of a COTS application software package to the development of a new AIS or infrastructure system.

a. AIS Development – AIS Development involves the development and deployment of an AIS to support a new or changed business function, replace an existing AIS which can no longer fulfill business needs, or to automate functions being done manually. Replacement of an existing AIS may include changing major components of the architecture.

b. AIS Enhancement – AIS Enhancements involve significant changes to the AIS design specification or architecture to ensure that new or changing requirements are being met.

c. AIS or Infrastructure Maintenance – AIS or Infrastructure maintenance are projects with new functionality changes or corrections (bug fixes) that do not impact the design or architecture of the AIS or infrastructure.

d. Infrastructure Development or Enhancement – Infrastructure Development or Enhancement involves the installation of new or replacement hardware or system software products such as the installation of high-speed switches or the upgrade of the network operating system. Infrastructure Development or Enhancement supports the evolution and adaptation of the USPTO Information Technology Infrastructure to support new systems and the increasing demands placed on it.

1.4 Life Cycle Management Phases

The LCM phases may be tailored to accommodate the unique aspects of an AIS or infrastructure system project as long as the resulting approach will deliver a quality system.

Life Cycle Management includes six phases, during which defined AIS or infrastructure system work products are created or modified. The tasks and work products for each phase are described in subsequent chapters. The LCM phases may be tailored[2] to accommodate the unique aspects of an AIS or infrastructure system project as long as the resulting approach remains consistent with the primary LCM objective to deliver a timely, quality system within cost. LCM phases may overlap and AIS or infrastructure system projects can follow an evolutionary development strategy that provides for incremental delivery of products and/or subsystems. The tailoring process is described in the Automated Information System Life Cycle Process Tailoring Technical Standard and Guideline, IT-212.2-03.

1.4.1 Initiation Phase

The purposes of the Initiation Phase are to:

a. identify and validate an opportunity to improve business accomplishments of the organization or a deficiency related to a business need,

b. identify significant assumptions and constraints on solutions to that need, and

c. recommend the exploration of alternative concepts and methods to satisfy the need.

This phase is completed upon agreement between the Program Sponsor and the Chief Information Officer (CIO) to initiate an AIS or infrastructure system project.

1.4.2 Concept Phase

This phase will determine whether an acceptable and cost-effective approach can be found to address the business need, with high confidence that technology can support it. The purposes of this phase are to:

a. identify system interfaces,

b. identify basic functional and data requirements to satisfy the business need,

[2] Tailoring is the process of omitting or reducing tasks and work products from the AIS or infrastructure system project management plan. In special cases, tailoring may add tasks or work products.

c. identify basic electronic records management requirements and ensure that the AIS or infrastructure system is compliant with the Federal Records Act, Privacy Act, and Paperwork Reduction Act,

d. establish system boundaries, identify goals, objectives, critical success factors, and performance measures,

e. evaluate costs and benefits of alternative approaches to satisfy the basic functional requirements,

f. assess project risks,

g. identify and initiate risk mitigation actions, and

h. develop high level architecture, process models, data models, a records schedule, and a concept of operations.

This phase may include several trade-off decisions such as the decision to use COTS software products as opposed to developing custom software or reusing software components, or the decision to use an incremental delivery versus a complete, one-time deployment. Construction of executable prototypes is encouraged to evaluate technology to support the business process. The Program Sponsor approves requirements and the Technical Review Board verifies that the requirements are clearly defined. This phase is completed upon approval by the Technical Review Board at the High Level Requirements Review and when the Program Sponsor and the CIO agree to the system boundary.

1.4.3 Detailed Analysis and Design Phase

The purposes of this phase are to:

a. further define and refine the functional and data requirements,

b. complete a retention schedule for records and obtain approval from the National Archives and Records Administration and ensure that electronic records management requirements are incorporated into the design,

c. complete reuse component selection,

d. complete business process reengineering of the functions to be supported,

e. develop detailed data and process models,

f. define functional and system requirements that are not easily expressed in data and process models,

g. further refine the high level architecture and logical design to support the functional and technical requirements, and

h. continue to identify and mitigate risks, coordinating with the business area to ensure that new technology can be phased in.

At the end of this phase, the system is described by a completed high level architecture and logical design. This phase is completed upon Technical Review Board approval at the Technical Design Review. The Technical Review Board records this approval in a record of agreement, as described in the Technical Review Board Charter.

1.4.4 Development Phase

The purposes of the Development Phase are to:

a. design, develop, integrate, and test the AIS or infrastructure system,

b. update and finalize plans to deploy the AIS or infrastructure system, and

c. complete business transition planning, and identify and initiate business transition activities.

All components of the logical design are allocated to components of the detailed design and detailed design is completed and transformed into a physical design. Risk identification and mitigation activities continue to be performed to address any remaining risk. This phase is completed when the Technical Review Board conducts the Production Readiness Review confirming that the AIS is complete, correct, fully tested, and ready for the Deployment Phase to begin.

1.4.5 Deployment Phase

The purposes of the Deployment Phase are to:

a. ensure that the AIS or infrastructure system is installed as planned and specified,

b. ensure that the users are trained,

c. ensure that the end users and supporting organizations are prepared to accept the system.

In this phase, the system is installed to support the intended business functions. Performance objectives have been identified, agreed to, and recorded in a Service Level Agreement[3] contained in the Operational Support Plan prior to going into operation.

[3] Service Level Agreements are contained in the Operational Support Plan and describe the services OCIO provides to another USPTO organization. Each service description includes OCIO's commitments in regards to providing the service and the other organization's responsibilities in regards to obtaining the service. The final document is approved by the CIO and his peer in the other USPTO organization.

Deployment occurs incrementally when logistics do not permit all the intended end users to receive the system at the same time. Deployment includes user notification, user training, installation of hardware, installation of software onto production computers, certification of data, and integration of the system into daily work processes. The deployment phase ends when all the intended users are first processing all the intended workload with the system, and the Program Sponsor and the CIO agree that the AIS or infrastructure system is fully operational.

1.4.6 Operations Phase

The purposes of this phase are to:

a. operate, maintain, and enhance the AIS or infrastructure system,

b. certify that the AIS or infrastructure system can process sensitive information,

c. conduct routine data base assessment to ensure data quality and optimal data base performance is maintained,

d. conduct periodic assessments of the AIS or infrastructure system to ensure the functional requirements are being satisfied, and

e. determine when the AIS or infrastructure system needs to be modernized, replaced, or retired.

1.5 Tailoring the Life Cycle

The LCM can be tailored to fit the unique needs of an AIS or infrastructure system project. The tailored process will be described in the AIS or infrastructure system Concept Brief and Quality Assurance Plan. The Concept Brief is an informational briefing presented to the Technical Review Board in the Concept Phase that provides the project description, life cycle tailoring agreement, schedule, and any project issues.

The tailored life cycle will contain only that which is necessary for the delivery of a quality system on time and within budget. Common sense should prevail.

As a tailoring example, LCM tasks and products can be reduced for an AIS project to install a COTS software product on the existing USPTO information technology infrastructure. The System Development Manager should consider the size, complexity, and scope of the AIS or infrastructure system project when preparing the AIS or infrastructure system Project Management Plan. During this phase, the System Development Manager will identify a tailored life cycle for the AIS or infrastructure system and provide the tailoring information to the Office of System Product Assurance for consulting purposes. The tailored process must include the Concept Phase which bases much of the information gathering on the information engineering planning and analysis approach. Some of the Concept Phase tasks and work products may be omitted as long as the resulting approach provides for delivery of a timely, quality, system within costs. There are a few essential tasks and work products that cannot be "tailored out" even when a COTS software product will be used:

a. succinct functional requirements,
b. USPTO standard data definitions,
c. records management,
d. adequate testing,
e. configuration management,
f. user training,
g. user manuals, and
h. operations, maintenance, and help desk documentation.

The AIS Life Cycle Process Tailoring TSG, IT-212.2-03, provides guidance for LCM tailoring. The tailoring information will be presented in the Concept Brief to the Technical Review Board for approval.

1.6 System Development Methodology

1.6.1 General

The system development methodology supports an integrated set of principles, procedures, practices, technical standards, and supporting tools that the USPTO has adapted for use in developing, modifying, and managing AISs or infrastructure systems.

The system development methodology supports an integrated set of principles, procedures, practices, technical standards, and supporting tools.

USPTO's methodology is described in a series of technical standards and guidelines publications[4]. These technical publications describe methods and procedures as well as documentation requirements (format and content) associated with developing an AIS or infrastructure system within the USPTO information technology infrastructure. The methodology defines the activities that are needed to build a system, the interfaces among those activities, and the products created as a result of those activities. Much of the AIS or infrastructure system analysis and design-level documentation will be captured and maintained in the Computer Aided Software Engineering (CASE) tool repository, and reused where practicable.

1.6.2 System Development Methodology Criteria

In order for the USPTO to build upon business process reengineering activities, share data and processes, and develop and maintain responsive automated information systems on time and within budget, a rigorous and proven system development methodology is needed that:

a. Supports an integrated set of formal techniques for the planning, analysis, design, and development of automated information systems on an enterprise-wide basis rather than on a project-wide basis.

b. Is business-driven and firmly anchored in the strategic planning of the business enterprise.

c. Supports business process reengineering and provides for storage of planning information relative to the business enterprise such as data and process models, critical success factors, process improvement, best practices, and business functions, goals, and objectives.

[4] The USPTO Technical Standards and Guidelines are downloadable and may be found at http://ptoweb/ptointranet/tsg/tsgindex.htm.

d. Is supported by a set of commercially available automated tools that facilitate applying the methodology and provide for a rigorous enforcement of the methodology's techniques and standards.

e. Is a data-centered design approach and provides techniques for formal data modeling and data administration.

f. Imposes a rigorous discipline that enforces a good structuring of data and application program code.

g. Supports techniques to identify processes and process improvements that are used many times in the enterprise so that designs and program code can be reused.

h. Emphasizes top management involvement to provide strategic direction and active program sponsor/customer participation throughout the life cycle.

1.7 Policies and Guidelines for the Management of Projects

The following policies and guidelines apply throughout the full AIS or infrastructure system life cycle, including maintenance, and enhancement of AISs or infrastructure systems. Further information on these policies and guidelines is contained in Chapters 2 through 7 of this manual.

Following these policies and guidelines will result in a high probability that a quality system will be successfully integrated with business processes and will continue to be used effectively.

1.7.1 Manage AIS Projects as Investments

Proposed AIS or infrastructure system projects will be clearly supported by detailed analyses of the project's expected costs and benefits; alternative solutions considered; potential programmatic and technical risks; and the AIS's or infrastructure systems' overall contribution to the business area's and USPTO's mission, goals, and objectives.

1.7.2 Emphasize Evolutionary Development and Incremental Delivery of Products

AISs or infrastructure systems will be developed emphasizing evolutionary development and incremental delivery of products and services. AIS or infrastructure system project plans should focus on providing the end user with usable products as early as practical.

1.7.3 Improve End-User Productivity

AISs or infrastructure system will simplify and reduce the effort required to handle administrative activities so that more employees can focus on program-related workloads. Each AIS should meet the following objectives:

a. Emphasize user friendliness over ease of technical design and application software development.

b. Provide easier, secure, reliable access to data.

c. Tailor management information reports to customer needs.

d. Provide automated tools to facilitate end user access to and use of data.

e. Provide readily available help within the application software and provide for computer based training modules.

f. Reduce the reliance on paper.

g. Provide easier, secure access and management to electronic records.

1.7.4 Encourage End-User Involvement

End-user participation and involvement throughout life cycle activities is crucial to the success of each AIS or infrastructure system and must be encouraged. For example, end users must participate early in the AIS project in order to obtain clear, validated functional requirements. Due consideration must be given to ensure that all internal, external, and legal customer requirements are adequately reflected in the automated solution.

1.7.5 Ensure that Adequate End-User Training is Provided

End-user training is essential in order for the AIS or infrastructure system to be effectively used. End-users must be provided with initial training to support a newly installed AIS or infrastructure system, and must receive all additional training necessary to effectively utilize AIS or infrastructure system modifications and enhancements.

1.7.6 Employ Matrix Management Techniques

Matrix management techniques should be used to recognize the complementary roles of functional users, AIS or infrastructure system developers, and other supporting organizations. The Project Manager reports to the Program Sponsor, and is responsible for coordinating end-user participation and managing functional requirements. Generally, the System Development Manager reports to the CIO and is matrixed to the Project Manager. The System Development Manager is responsible for coordinating development and technical support, and for managing technical requirements.

1.7.7 Comply with USPTO Information Technology Standards and Guidelines

AIS or infrastructure system projects must follow the provisions of the USPTO Information Technology Standards and Guidelines (TSGs)[5], which provides up-to-date technical guidance designed to aid the System Development Manager deliver a quality system and the System Maintenance Manager to maintain and enhance one.

1.7.8 Use USPTO Information Technology Infrastructure and Ensure Compatibility With USPTO Technical Reference Model

AIS or infrastructure system projects must be developed within the bounds of current and planned information technology standards and capabilities as defined in the USPTO Strategic Information Technology Plan and USPTO Technical Reference Model[6]. An AIS or infrastructure system project's computer and network resource requirements must be satisfied by the USPTO information technology infrastructure capabilities whenever practicable. PTOnet and distributed processing platforms will be exploited to provide managers and staff with needed automated support.

A key information technology management objective is to transform the USPTO information technology infrastructure into a standards-based open system environment. An open system environment will allow the USPTO to add new or replace existing products or infrastructure components as new technologies are introduced into the marketplace. System Development Managers will select standards and products that conform to the Technical Reference Model in the detailed design and development of the technical architecture. System Development Managers must adhere to approved standards and preferred products unless other standards or products can be clearly demonstrated to be cost-effective over the life of the application.

The System Architect is responsible for developing, maintaining and evolving the USPTO information technology infrastructure and the USPTO Technical Reference Model.

1.7.9 Use USPTO Standard Data Definitions

Standard definitions of data will be developed and maintained so that it will be easier for users to reliably and consistently interpret and use data. AISs or infrastructure systems

[5] USPTO Technical Standards and Guidelines may be found at http://ptoweb/ptointranet/tsg/tsgindex.htm.

[6] The USPTO Strategic Information Technology Plan documents the role that information technology plays in achieving the USPTO's mission, vision, and goals. The USPTO Technical Reference Model provides a comprehensive set of information technology standards, services, protocols, and products that define the target technical environment for the acquisition, development, and support of USPTO AISs.

shall be developed using USPTO standard data models and data elements. Guidance is contained in the USPTO Data Management Technical Standard and Guideline, IT-212.2-05, and Data Element Standardization Technical Standard and Guideline, IT-212.3-13.

1.7.10 Use USPTO Standard System Development Tools

The CIO has selected a standard suite of system development tools that support the system development life cycle. The standard tools will reduce maintenance costs, make projects more predictable, reduce dependence on original developers, leverage the experience of in-house staff to work on different projects without retraining on system development tools, and facilitate reuse of software components. System Development Managers will use the USPTO standard system development tools designated in the USPTO Technical Reference Model and refrain from using other system development tools unless it can be clearly demonstrated that other system development tools would be more cost effective over the life of the application.

1.7.11 Cost and Schedule Performance Must Be Planned and Reported

USPTO has established a project management control system to provide visibility into actual progress of each project. The project management control system provides for tracking actual cost and schedule performance against project plans. This visibility will help both functional and technical managers identify problem areas and take corrective actions when actual results deviate significantly from plans. Project Managers and System Development Managers will ensure that the necessary information for each AIS or infrastructure system project is provided in a timely manner and entered into the project management control system. Project planning specialists from the CIO's Office of Technical Plans and Policy will assist the Project Manager and the System Development Manager in developing a project management plan and project schedule. The USPTO Project Management Technical Standard and Guideline, IT-212.2.01 provides guidance on how to prepare project management plans and project schedules.

1.7.12 Each Project Must Be Consistent with the USPTO Strategic Information Technology Plan

AIS or infrastructure system projects will be contained in the USPTO Strategic Information Technology Plan. New projects must be consistent with the USPTO Strategic Information Technology Plan and be agreed to by both the business area Program Sponsor and the CIO, as described in paragraph 1.4.1. The Program Sponsor and the CIO will identify and allocate project resources and the new project will be included in the next planning cycle. Project Managers shall identify in the LCM documentation the specific key goals and objectives of the USPTO Strategic Plan that are supported by the AIS or infrastructure system project.

1.7.13 Use of COTS Software is Encouraged

Commercial-Off-The-Shelf application software products cover a broad spectrum of capabilities. These products can satisfy USPTO business needs and can operate on USPTO's Information Technology Infrastructure. COTS application software products are preferred over developing new application software. USPTO unique requirements not provided by the COTS product will be satisfied through application program interfaces.

1.7.14 Business Processing Reengineering Techniques May Be Applied

USPTO will employ reengineering and continuous quality improvement techniques as required to help ensure that processes are as effective and efficient as possible. Information technology is a key enabler of process improvement. No AIS or infrastructure system project will be undertaken before the supported process has been reviewed and, as necessary, redesigned to its greatest possible effectiveness. If needed, formal business process reengineering will precede application software design and development. The business area Program Sponsor, in consultation with the CIO, will designate AIS or infrastructure system projects that will apply business reengineering techniques.

1.7.15 Secure and Protect All Sensitive Information

Security of all sensitive information must be explicitly considered throughout the AIS or infrastructure system life cycle and documented in an AIS security and disaster recovery plan. Program Sponsors, with the guidance and assistance of the CIO, must ensure that their AISs or infrastructure system and business procedures will process and handle sensitive information and deliver critical services in a manner compliant with all applicable laws and regulations. AISs or infrastructure systems will be controlled with respect to access, authority to modify, and ability to operate. Security specialists from the CIO's Office of Technical Support Services will maintain a USPTO Information Technology Infrastructure Security and Disaster Recovery Plan and assist the System Development Manager develop a security and disaster recovery plan that addresses the unique business requirements of an AIS or infrastructure system project.

1.7.16 Apply Risk Management Techniques

Risk management must be applied to all LCM-AIS projects throughout the life cycle. Risk, as used in the LCM, is associated with a lack of resources, information, and/or control. Risk management is distinguished from "problem management" in that risk management is concerned with situations that may or may not occur, whereas problem management is concerned with known difficulties that are a result of a risk having occurred. An analysis of risk and any strategy adopted to control risk should at least consider the effect of one or more of three factors: lack of resources (such as personnel or funding); lack of information (for example, completeness and confidence); or lack of control over the decision-making process (such as external project decisions affecting the project plans and assumptions). Applying risk management to production AISs or infrastructure systems includes considering backup and recovery in service level agreements and plans. Management responsibility for a risk must be assigned to individuals and organizations that can affect the risk's root causes. The Project Manager shall be responsible for managing project risks over which the Project Manager can exert direct control. Risks that affect the project, but are not under project control, shall be explicitly assigned to either the Program Sponsor or the CIO, as appropriate. Situations external to the project that could be sources of risk to the project shall be coordinated through the Project Manager. Risk shall be a consideration in Technical Review Board and management decisions. Project risk situations, plans, and progress against risks must be considered at all project reviews. Guidance is contained in the USPTO Project Management Technical Standard and Guideline, IT-212.2-01.

1.7.17 Focus on Software Process Improvement

The USPTO is committed to a program of continuous software process improvement. The USPTO's software process improvement program will enhance the USPTO's ability to deliver quality systems in a timely and cost-effective manner. Established in January 1994 to define and institutionalize a USPTO-standard system development life cycle management process, the Software Engineering Process Group (SEPG) is the CIO's focus group for capturing best practices, presenting new technology and tools, reviewing draft guidelines and keeping the CIO staff aware of new software process improvement opportunities. System Development and System Maintenance Managers must stay abreast of and contribute to process improvements in order to institutionalize LCM within USPTO and make it work.

1.7.18 Manage AIS or Infrastructure System Baselines

An AIS or infrastructure system baseline is an approved set of work products for a stage in the system life cycle. Baselines are established at the completion of phases of the life cycle. The set of work products designated as a baseline is managed as a unit. Changes to baselines are approved by their designated owners. System Development and System Maintenance Managers must establish and maintain baselines throughout the AIS or infrastructure system life cycle to: keep successive versions of the system synchronized with incremental service delivery promises; keep track of the current contents of the complete systems; and maintain complete technical data packages. Properly managing baselines will prevent costly later rework and rediscovery, and aid reuse. Configuration management specialists will periodically audit established AIS or infrastructure system baselines to verify that they conform to the documentation that defines them. The Configuration Management Technical Standard and Guideline, IT-212.2-06, describes the baselines and their contents in more detail. Technical reviews decide completion, and each baseline type is described in Section 1.8.2, Conducting Technical Reviews.

1.7.19 Implement Key Software Management Processes

The following policies apply to phase-independent key software process areas that are necessary to support the definition, design, development, deployment, operation, maintenance, and enhancement of AISs or infrastructure systems. These key process areas are configuration management, quality assurance, data management, and requirements management. Other key process areas are discussed in the relevant chapters of this Manual.

a. Requirements Management. Requirements management controls the identification, definition and refinement of requirements as analysis proceeds from high level to detail definition, and allocation to system and subsystem components. Requirements must be managed as they change and evolve throughout the AIS or infrastructure system life cycle. The System Development Manager will create and maintain a requirements database and a requirements traceability matrix to identify changes throughout the AIS or infrastructure system life cycle. Requirements management specialists from the Office of System Product Assurance will help the System Development Manager develop the requirements traceability matrix.

b. Data Management. The System Development Manager will establish plans to manage the data, data models, and databases required by the AIS or infrastructure system. Data management plans will be defined and updated to ensure that all data related issues are addressed throughout the life cycle and to ensure that the agency records management program is followed for compliance with records management laws and regulations. Data management specialists from the CIO's Office of Data Management will, in coordination with the System Development Manager, prepare data management plans and will review the data management plans and data models to ensure compliance with data administration policy and guidelines. Data management specialists will also facilitate the processes for developing data models and standardizing data elements. Records management staff from the CIO's Office of Data Management will assist the System Development Manager in scheduling AIS or infrastructure system records and ensure that the AIS or infrastructure system is compliant with the Federal Records, Privacy Act, and Paperwork Reduction Act and meets basic electronic records management requirements.

c. Quality Assurance. The System Development Manager will establish plans to provide management with appropriate visibility into the process being used by the software project and the products being built. Quality assurance specialists from the Office of System Product Assurance will, in coordination with the System

Development Manager, prepare Quality Assurance plans and will attend all major technical reviews. Quality assurance specialists will review and audit the AIS or infrastructure system project work products and activities to help assure that the AIS or infrastructure system Project will deliver a quality system.

d. Configuration Management. Configuration management of all AIS or infrastructure system hardware, software, and accompanying documentation shall be performed throughout the AIS or infrastructure system life cycle. The Office of System Product Assurance, in coordination with the System Development Manager, will establish plans and baselines to ensure configuration identification, configuration control, configuration status accounting, and configuration audits for all configuration documentation, physical media, and physical parts composing the system. Configuration management shall also be applied to any resources such as compilers or CASE tools used to develop the AIS or infrastructure system. The configuration management process shall provide a means for recording, reviewing, approving, and tracking change requests and problem reports for all configuration items/units. Configuration management methods will be compatible with and leverage the use of standard system development tools designated in USPTO's Technical Reference Model. Configuration management specialists from the Office of System Product Assurance will work with the System Development Manager in preparing configuration management plans and performing configuration management and will attend all major technical reviews.

1.7.20 Conduct Peer Reviews

Peer reviews will be conducted on designated critical AIS or infrastructure system projects to identify and remove defects from the project's work products early and efficiently. The AIS or infrastructure system project's peer review process and the specific work products that will undergo peer review will be documented in the quality assurance plan. Peer reviews should be led by trained peer review leaders, and each person attending a peer review will have a specific role that they are trained to perform. Products that undergo peer review will have all actions identified as a result of the peer review tracked until they are resolved. Checklists that guide the peer reviews will be maintained by the Office of System Product Assurance, and reviewed by the checklist's potential users. Results of peer reviews will be collected and reported in a manner that leads to positive corrective actions taken and not to evaluate the performance of individuals.

1.7.21 Establish A Technical Training Program

A technical training program for the AIS or infrastructure system project must be established to help ensure that appropriate skills and knowledge of individuals assigned to the project are developed so that they can perform their project roles effectively and efficiently. Each project will evaluate its current and future skill needs and determine how these skills will be obtained. Technical training specialists from the CIO's Office of Technical Plans and Policies will assist the System Development Manager in developing a training program.

1.7.22 Encourage Prototyping

The use of prototyping in the Concept and Detailed Analysis and Design Phases to help define and refine requirements is encouraged. Prototypes can enhance user and developer understanding and interpretation of requirements or validate portions of the technical architecture against the functional requirements and technical specifications. Executable prototypes must be fully tested and documented and meet the minimum criteria established in section 1.5 prior to being placed in pilot or production status. Additional information on prototyping and pilots[7] is provided in chapters 3 and 4 of this document.

1.7.23 Reuse Software Whenever Practical

The reuse of existing system components will reduce cost and quicken system delivery. System Development Managers will construct AISs or infrastructure systems from previously developed system components whenever practical. The reusable components include data and process models, technical design specifications, plans, test suites, and program code.

1.7.24 Help Ensure Software Independence

AISs or infrastructure systems will be developed, documented, and maintained in such a manner as to reduce reliance on individuals or organizations that operate, maintain, or enhance the AIS or infrastructure system. Initially, this will require additional cost and effort to collect, analyze, and enhance the life cycle documentation necessary to ensure software independence. Once this technical knowledge base has been firmly established, however, AISs or infrastructure systems can be maintained and enhanced much more cost-effectively, much faster and with far less effort.

[7] Pilot - A limited scope application program that satisfies most, if not all of the user's requirements. It normally is targeted to a limited user group for evaluation with the understanding that it will be scaled up and integrated into a fully compatible production system.

1.7.25 Using Contractor Support

For contractor-supported AIS or infrastructure system projects, System Development Managers will ensure that USPTO personnel work closely with the contractor to ensure that tasks are accomplished in a quality, timely, and cost-effective manner and that technology transfer occurs. Contractors are prohibited from preparing Project Manager Charters and related decision memoranda. Contractors are also prohibited from assigning a role, responsibility or authority, which is documented in the Project Management Plan.

1.7.26 Maintain Complete Project Records

LCM documentation developed in support of AIS or infrastructure system projects will be retained in accordance with USPTO's record management schedule. LCM documentation developed in support of an AIS or infrastructure system project that is retired before successful fielding also will be retained in accordance with USPTO's record management schedule. All documentation related to a contract shall be retained after contract close-out in accordance with USPTO's record management schedule. Contract close-out is the last billing date and may be as long as 3 years after the end of the contract.

1.8 AIS or Infrastructure System Project Reviews

Diverse and rapidly developing opportunities to employ computers to improve mission performance have brought increased importance to the application and management of information technology. Technical reviews must be performed to ensure that an AIS or infrastructure system project is progressing on schedule and within budget and is satisfying functional requirements. The conduct of the reviews may be tailored to address the specific needs of each project consistent with the development plan. The Technical Review Board conducts reviews of work products and plans for the next life cycle phase. The CIO conducts in-progress reviews of cost, schedule and deliverables. The Program Sponsor and the CIO jointly conduct a management review to decide to initiate an AIS or infrastructure system project.

Technical reviews provide a mechanism to help managers monitor the progress of an AIS or infrastructure system project and direct corrective actions to keep the project on schedule for delivering a quality system.

1.8.1 Purpose of Technical Reviews

Technical reviews are performed to provide sufficient visibility into the AISs or infrastructure systems' functional and technical characteristics, as well as establish management control points for assessing project cost, schedule, and quality. The purposes of a technical review are to:

a. Improve the quality of intermediate AIS or infrastructure system work products and to correct defects as early in the life cycle as possible in order to prevent problems over the long run.

b. Ensure that the AIS or infrastructure system being produced can be supported by the current and planned USPTO information technology infrastructure.

c. Ensure that the AIS or infrastructure system project conforms to USPTO system development methodology and supporting tools, uses USPTO standard data, and adheres to the USPTO Technical Reference Model.

d. Monitor the impact of an AIS or infrastructure system project on other USPTO AISs, AIS projects, and the USPTO information technology infrastructure.

1.8.2 Conducting Technical Reviews

The Project Manager, System Development Manager, or Technical Review Board Chairperson may choose to convene technical reviews at any time during the life cycle to determine the state of work products. Technical reviews may be held as one or more events as determined by the Technical Review Board Chairperson. Reviews may be combined. The conduct of the reviews may be tailored to address the specific needs of each project consistent with the AIS or infrastructure system development plan. Tailoring guidance may be found in the Automated Information System Life Cycle Process Tailoring Technical Standard and Guideline, IT-212.2-03. A typical project will not require all the reviews and baselines discussed below. Guidance is contained in the USPTO Quality Assurance Technical Standard and Guideline, IT-212.2-04.

a. High Level Requirements Review. This review is conducted to confirm that a common understanding of the functional requirements for the AIS or infrastructure system is captured in the System Boundary Agreement or Requirements Specification, Part 1. This review is conducted at the end of the Concept Phase. This review approves the System Boundary Baseline, which includes the functional requirements and project related cost, schedule, and performance measures. The System Boundary Baseline contains the System Boundary Agreement. The developmental configuration is initiated after this review under the ownership of the System Development Manager. The developmental configuration consists of the design and the associated technical data that defines the components of the system.

b. Detailed Level Requirements Review. This review is conducted to confirm that a common understanding of the functional requirements for the AIS or infrastructure system is captured in the Requirements Specification, Parts 1 and 2[8]. This review is conducted during the Detailed Analysis and Design Phase. This review approves the Requirements Specification, Parts 1 and 2.

c. Logical Design Review. This review is conducted during the Detailed Analysis and Design Phase to confirm the functional, data and other requirements of the AIS, to verify the data and process models of the AIS or infrastructure system, to confirm the ability of the High Level Architecture to satisfy the functional, data and other requirements and to confirm the allocation of requirements to components of the technical architecture. This review approves the logical design (allocated) baseline, which describes approved functional, data, interface, and other requirements allocated to the system or subsystem elements.

d. Technical Design Review. This review is conducted during the Detailed Analysis and Design Phase to evaluate the appropriateness of the technical design. This

[8] The Requirements Specification organizes the requirements into high level (Part 1) and detailed requirements (Part 2).

review verifies that the system conforms to the infrastructure baseline. The USPTO Information Technology Infrastructure is controlled separately from any individual AIS project. This baseline is managed by the System Architect.

e. Test Readiness Review. This review is conducted at the end of the Development Phase to determine whether unit and integration testing has been conducted in accordance with the test procedures and that the tests are complete. This review determines whether the system is ready for independent acceptance testing. The development configuration is created during the Development Phase and maintained under informal configuration management at the project level until the end of the Development Phase. The developmental configuration consists of the design and associated technical data that defines the components of the system. A version of the Developmental Configuration is placed under formal configuration management after Test Readiness Review and is used for acceptance testing.

f. Beta Readiness Review. This review is conducted during independent acceptance testing to determine whether formal testing is complete and the system is ready for user Beta testing. The review is performed during the Development Phase.

g. Production Readiness Review. This review is conducted at the end of the Development Phase to determine whether the system is adequately tested, satisfies the boundary conditions, and is ready for production use. The Program Sponsor participates in the Production Readiness Review. This review establishes that appropriate operational and maintenance support is available. This review establishes the product and operational baselines. The Product Baseline consists of the documentation describing all the necessary functional and physical characteristics of the elements that compose the system and the actual equipment and software. The Operational Baseline consists of the parameters and procedures needed to operate and to perform routine maintenance on the AIS or infrastructure system. The Operational Baseline is established to record changes to those items for which a review by the Technical Review Board prior to making the change is not required.

h. Post Installation Review. This review assesses results during the production trial period. The TRB or the Project Manager may request that a Post Installation Review (PIR) be conducted. The PIR is used to identify remaining discrepancy reports, deferred requirements for future maintenance releases, and any issues related to the system operation. Based upon the results of this review, the Technical Review Board and the business area Program Sponsor give permission for the AIS or infrastructure system to remain in production if there are no serious problems.

i. Functional Configuration Audit. This audit may be conducted during the Deployment Phase to ensure that all functional requirements specified in the System Boundary Agreement are satisfied.

j. Physical Configuration Audit. This audit is conducted during the Deployment Phase to determine whether the delivered ("as built") system is complete and consistent with its documentation.

1.8.3 In-Progress Reviews

The CIO and Program Sponsors conduct periodic in-progress reviews (IPR) to assess progress, adherence to schedule and budget, possible impact on other projects, and to direct corrective actions as needed. Project Managers and System Development Managers should also hold regularly scheduled (e.g., biweekly) project status reviews that discuss progress against project plan as well as technical issues.

1.9 Roles and Responsibilities for AIS or Infrastructure System Project Management

The successful development, deployment, and operation of an AIS or infrastructure system require close coordination and partnership between the Program Sponsor and the CIO. Teamwork is essential to delivering a quality system on time and within budget. The Program Sponsor identifies and prioritizes business needs. The CIO determines how best to employ technology. The Program Sponsor and the CIO provide resources and work together to determine the project schedule and cost estimates.

The successful development, deployment, and operation of an AIS or infrastructure system require close collaboration and partnership between the Program Sponsor and the CIO.

1.9.1 Program Sponsor

The Program Sponsor is responsible for defining and validating functional requirements, for making resources available to support information technology program initiatives, and for reviewing the progress of AIS or infrastructure system projects to ensure that functional requirements are being satisfied in a timely and cost-effective manner. Program sponsors within their area of responsibility will:

a. Ensure that the goals and objectives of all information technology related initiatives are consistent with the goals, objectives, and governing strategies of the USPTO Corporate Performance Plan and the Business Area's Strategic Plan.

b. Exercise management oversight of AIS or infrastructure system projects to ensure that business requirements are being satisfied in a cost-effective manner.

c. Exercise management oversight of the evaluation and improvement of business processes as well as the development of business goals, objectives, critical success factors, and performance measures.

d. Ensure that the necessary data for each AIS or infrastructure system project are provided in a timely manner and are entered into USPTO's project management control system and work with the CIO to ensure that corrective actions are taken when needed.

e. Ensure, with the assistance of the CIO, that AISs or infrastructure systems processes handle sensitive information and deliver critical services in a manner compliant with all applicable laws and regulations.

f. Ensure that business area transition planning and appropriate training are accomplished in a timely manner.

g. Assign Project Managers to direct and coordinate the complete effort to achieve agency business objectives to be accomplished by the AIS or infrastructure system project.

h. Assign Production Managers to direct and coordinate the maintenance and modifications of an operational AIS or infrastructure system required to keep up with changing business needs.

1.9.2 Chief Information Officer (CIO)

The CIO is the principal advisor to the Commissioner on the effective application of information technology and will:

a. Ensure that all information technology initiatives are managed in accordance with sound life cycle management principles and practices and are consistent with the USPTO Strategic Information Technology Plan.

b. Perform technical reviews to ensure that an AIS or infrastructure system project is progressing on schedule and within budget and is satisfying functional requirements.

c. Establish service level agreements to promote organized and timely information technology support to customers.

d. Use the results of periodic customer focus sessions to identify opportunities for improvement, to determine customer needs, and to determine whether an AIS or infrastructure system effectively serves its users and meets established performance measures.

e. Establish and administer a project management control system to provide visibility into the actual progress of each AIS or infrastructure system project.

f. Ensure that security is adequately considered in system design and issue an accreditation statement that authorizes operation of the AIS or infrastructure system based on evidence provided by the certification and verified by an accreditation audit.

g. Assign a System Development Manager to develop and deploy an AIS or infrastructure system.

h. Assign a System Maintenance Manager to perform system maintenance and develop and deploy system enhancements as identified and prioritized by the Production Manager.

i. Operate the AIS or infrastructure system according to established Service Level Agreements contained in the Operational Support Plan.

1.9.3 Steering Committee

The Steering Committee may be created to perform the duties of or assist the Program Sponsor when an AIS or infrastructure system project crosses organizational boundaries. The Steering Committee is composed of functional and technical representatives appointed by the Program Sponsor and the CIO.

1.9.4 Project Manager

Appointed by the Program Sponsor, the Project Manager oversees the complete effort to achieve agency business objectives to be accomplished by the AIS or infrastructure system project. The Project Manager, in coordination with the Program Sponsor, the System Development Manager, and other managers, develops the project budget and schedule, and monitors cost and schedule performance for the project. The Project Manager will:

a. Provide daily direction and coordination for the business aspects of the design, development, and deployment of an AIS or infrastructure system subject to the technical direction of the CIO and the business direction of the Program Sponsor.

b. Coordinate changes to the business environment brought on by the implementation of new business processes. The changes to the business environment may require resolution of labor management issues, legal issues, employee relations issues, and/or changes to the physical workplace environment.

c. Ensure that users: (1) actively participate in the AIS or infrastructure system project to help identify and refine requirements and to test the system; and (2) are adequately trained before the AIS or infrastructure system is fully deployed.

d. Under matrix management, the Project Manager directs the activities of the project team. The Project Management Technical Standard and Guideline, IT-212.2-01, describes the responsibilities of the Project Manager in more detail.

1.9.5 System Development Manager

Appointed by the CIO, the System Development Manager is responsible for designing, developing and deploying an AIS or infrastructure system. The System Development Manager ensures that the AIS or infrastructure system is consistent with the agency's strategic information technology plans and is managed according to sound life cycle management principles and practices. The Project Management Technical Standard and Guideline, IT-212.2-01, describes the responsibilities of the System Development Manager in more detail.

1.9.6 System Architect

A senior manager in the Office of System Architecture and Engineering serves as the USPTO System Architect. Appointed by the CIO, the System Architect is responsible for:

a. Developing or approving the high level design for all USPTO AISs or infrastructure systems,

b. Managing the evolution of USPTO's information technology infrastructure, and

c. Developing and maintaining the USPTO's Technical Reference Model.

The Technical Reference Model provides a comprehensive set of information technology standards, services, protocols, and preferred products that define the target technical environment. This model is used for the acquisition, development, and support of all USPTO AISs or infrastructure systems.

1.9.7 Production Manager

Appointed by the Program Sponsor, the Production Manager, directs and coordinates the maintenance and modification of an operational AIS or infrastructure system required to keep up with changing business needs. Under matrix management, the Production Manager identifies and prioritizes functional requirements that will be incorporated into an operational AIS or infrastructure system by the System Maintenance Manager and coordinates the implementation of those changes in the business environment. The

Production Manager ensures that users participate in system testing and are adequately trained before the AIS or infrastructure system changes are fully deployed. The Production Manager assures that the AIS or infrastructure system has been adequately secured.

1.9.8 System Maintenance Manager

Appointed by the CIO, the System Maintenance Manager performs system maintenance and develops and deploys system enhancements as identified and prioritized by the Production Manager. The System Maintenance Manager ensures that the operational AIS or infrastructure system is managed according to sound life cycle management principles and practices.

1.9.9 Technical Review Board

Appointed by the CIO, the Technical Review Board evaluates the progress of each AIS or infrastructure system project by assessing the quality of its work products and recommends action to the CIO. The Board ensures that USPTO's Life Cycle Management methodology is followed in a coordinated, common-sense manner for all AIS or infrastructure system projects by conducting technical reviews described in section 1.8. Results of the technical reviews are provided to the Commissioner of Patents and Commissioner of Trademarks, as appropriate. The Technical Review Board Charter defines the Board's authority and responsibility in more detail.

1.9.10 Software Engineering Process Group

Appointed by the CIO, the Software Engineering Process Group defines, introduces, monitors, and continuously improves system development life cycle processes. The goal of the SEPG is to develop and institutionalize an identifiable, measurable, and repeatable life cycle management process that facilitates the delivery of quality systems when promised and within cost estimates. The Software Engineering Group Charter defines the Group's authority and responsibility in more detail.

DETAILED ANALYSIS and DESIGN PHASE

4.1 Introduction

4.1.1 Purpose

During the Detailed Analysis and Design Phase, the Project Manager and the System Development Manager work closely together to:

a. Complete business process engineering of the functions to be supported,

b. Complete component selection.

c. Develop detailed data and process models,

d. Refine functional and system requirements that are not easily expressed in data and process models,

e. Refine the high level architecture and logical design to support the system, functional, and electronic records management requirements,

f. Continue to identify and mitigate risk that the technology can be phased-in and coordinated with the business.

There are three key reviews during the Detailed Analysis and Design Phase: the Detailed Level Requirements Review, Logical Design Review, and the Technical Design Review. This phase is completed when the Technical Review Board approves the high level architecture and system requirements, revised economic analysis, the logical design including the business process description, and the technical design. This approval is provided at these three reviews.

4.1.2 Overview

Detailed logical models of business data and processes needed to guide system development are created in the Detailed Analysis and Design Phase, and a description of the technical architecture is refined to guide the allocation of computing resources and capabilities. When practicable, the deployment of the new AIS should be planned to coincide with the implementation of new business processes and procedures. The Project Manager and the System Development Manager should continue to assess both business and technical

When practicable, the deployment of the new AIS should be planned to coincide with the implementation of new business processes and procedures.

risks and seek additional management support as necessary to manage those risks. Both the Project Manager and the System Development Manager may wish to document project risks and risk management activities in a risk management matrix for future reference.

4.1.3 Tasks

The primary tasks performed during the Detailed Analysis and Design Phase are as follows:

a. Consolidate and affirm business needs,

b. Implement AIS project management infrastructure including requirements, configuration, and data management support services and utilities,

c. Revise plans to document changes in project scope including changes in business, schedule, and technical requirements,

d. Revise plans to document changes in available resources including budget, skills, staff, and training,

e. Update list of candidate reuse components, and complete reuse component selection.

f. Complete electronic records management requirements,

g. Identify data acquisition, conversion, and validation strategies,

h. Refine the technical architecture and build architectural prototype,

i. Identify design tools, techniques, and procedures,

j. Perform detailed AIS analysis and design, and

k. Continue planning for AIS testing, training, deployment, operation and business transition, and

l. Define and refine detailed requirements and allocate requirements to design.

4.1.4 Activities and Documentation

Detailed Analysis and Design Phase activities and documentation requirements as summarized in the following table must conform to the indicated Technical Standard and Guidelines or other standards as noted.

The set of system requirements that satisfies the Business Case is contained in the Functional Baseline as indicated under the "Functional" subheading in Table 4.1.4.

Work products and design documents included in the Logical Design (Allocated) Baseline are identified under the "Logical Design" subheading in Table 4.1.4.

The Configuration Management TSG, IT-212.2-06, provides additional information about these baselines. Published standards and guidelines may be augmented with Tailoring Agreements.

						Baseline		
Work Product	TSG/ Standard	Who's Responsible	Must Create	Should Update	Must Update	Functional	Logical Design	Must Complete
Business Case	IT-212.2-13	Program Sponsor, Project Manager			X			
Project Management Plan and supporting baseline project schedules	IT-212.2-01	Project Manager, System Development Manager			X			
AIS Project Quality Assurance Plan	IT-212.2-04	Office of System Product Assurance		X				
Data Management Plan	IT-212.2-05	Office of Data Management			X			
AIS Configuration Management Plan	IT-212.2-06	Office of System Product Assurance		X				
System Boundary Agreement	IT-212.2-10	Project Manager, System Development Manager			X		X	X
Concept of Operations	IT-212.2-11	Program Sponsor, Project Manager			X	X	X	
Detailed Design (includes data model, screen shots and report layouts)	IT-212.2-12	System Development Manager, System Architect	X			X	X	
Interface Design Definition	IT-212.3-14	System Development Manager	X					X
Economic Analysis	IT-212.2-13	Project Manager, System Development Manager			X			
Business Transition Plan	IT-212.3-05	Program Sponsor, Project Manager	X					X
Requirements Specification, Part 2 (Completed through lower level requirements)	IT 212.3-11	Project Manager, System Development Manager	X		X		X	

						Baseline		
Work Product	TSG/ Standard	Who's Responsible	Must Create	Should Update	Must Update	Functional	Logical Design	Must Complete
Requirements Traceability Matrix	IT-212.3-11	Office of System Product Assurance	X				X	
Test Plan	IT-212.3-01	Office of System Product Assurance	X					X
Training Plan	IT-212.3-02	Project Manager, System Development Manager	X					X
AIS Security Plan (only if sensitive data)	IT-212.2-08	Project Manager, System Development Manager			X		X	
Operational Support Plan	IT-212.5-01	Project Manager, System Development Manager	X					X

Table 4.1.4 Detailed Analysis and Design Phase Activities and Documentation Requirements (Concluded)

4.2 Detailed Requirements Analysis

Business requirements are intended to state in a concise, complete, and unambiguous manner what the system must do to meet business needs.

Business requirements are intended to state in a concise, complete, and unambiguous manner what the system must do to meet business needs. Business requirements should not introduce unnecessary design assumptions or technical constraints. In this phase, the high level data and functions defined in the Concept Phase are transformed into a detailed description from which the system can be developed. This description will use a combination of textual and graphical representations to express the requirements in a form that users can readily understand. The functional, data, and support requirements must be approved by the Program Sponsor. Direct involvement of supported users and business area experts is essential to developing functional and data requirements. See IT-212.3-11, Requirements Management, for a description of the requirements definition process and documentation requirements.

4.2.1 Functional and Data Requirements Definition

Complete, user-oriented functional and data requirements for the system must be analyzed, defined, and documented. Screens, reports, and diagrams are useful in documenting the functional and data requirements. Analysis, definition, and documentation of requirements ensures :

a. All requirements can be traced to the System Boundary Agreement and Concept of Operations.

b. Business process descriptions contained in the Concept of Operations are further refined. The detailed design is captured in the Detailed Design Document and must be consistent with the Concept of Operations.

c. Reuse of existing USPTO software components is based on the list of candidate components. Components identified in the USPTO reuse repository should be evaluated against the AIS requirements to determine if the component meets the system needs as-is, requires a defined set of enhancements, or is incompatible with the AIS requirements.

d. The USPTO reuse repository is extended by selecting candidate components to be developed in parallel with the AIS development effort. For each component selected, a component specification should be defined to document the services offered by the component.

e. A logical model is constructed that describes the fundamental processes and data needed to support the desired business functionality. This logical model will show how processes interact and how processes create and use data. These processes will be derived from the activity descriptions provided in the System Boundary Agreement and Concept of Operations. For projects involving migration, old data elements should be mapped to new data elements.

f. Functions and entity types contained in the logical model are extended and refined from those provided in the Concept Phase. End-users and business area experts will evaluate all identified processes and data structures to ensure accuracy, logical consistency, and completeness.

g. An analysis of business activities and data structures is performed to produce work products such as, entity-relationship diagrams, process hierarchy diagrams, and process dependency diagrams.

h. A detailed analysis of the current technical architecture, application software, and data is conducted to ensure that limitations or unique AIS requirements have not been overlooked.

These requirements must include considerations for capacity and growth. Where feasible, the I-CASE tool will be used to assist in this analysis, definition, and documentation.

4.2.2 Support Requirements

Additional requirements that affect the design or use of the system must be defined in the Detailed Analysis and Design Phase as indicated below.

a. Functional and technical training needed for development, deployment, and operation of the AIS, including associated training schedules and costs, must be coordinated with the business area training representative, system users, and training organizations, such as the Work Force Effectiveness Division and the Patent Academy, in a timely manner. Section 6.6 provides additional information on training.

b. Requirements for logistical and network support needed to develop, deploy, and operate the AIS are identified in this phase and are documented in the Detailed Design and in the Operational Support Plan. These documents may be updated during follow-on phases.

c. AIS review, testing, evaluation, certification, and security requirements are identified, including associated schedules and costs. Timely coordination with all support organizations involved in addressing these requirements must be provided, particularly for independent, third-party organizations.

d. Plans needed to support system development, deployment, training, operation, and maintenance must be developed and coordinated with system users and support organizations, and must be implemented in a timely manner.

e. The justification for developing or enhancing an AIS application must always be expressed in business terms. The specific business needs that must be addressed are referred to as "performance requirements." In addressing performance requirements, project management is able to demonstrate that the AIS addresses a set of real business needs and objectives. Performance requirements focus on improving customer satisfaction, work force accuracy, productivity, responsiveness, and reliability.

4.2.3 Requirements Traceability

Requirements will be captured in a requirements traceability matrix as described in the Requirements Management TSG, IT-212.3-11 for designated AIS projects. This matrix must show the traceability of the detailed requirements contained in the Requirements Specification, Part 2 to the Detailed Design Document The high level requirements are recorded in the System Boundary Agreement, the Concept of Operations, and the Requirements Specification, Part 1.

4.2.4 Detailed Level Requirements Review

The products of the detailed requirements analysis are reviewed by the Technical Review Board at the Detailed Level Requirements Review. The purposes of this review are to:

a. Confirm functional and data requirements,

b. Review the candidate component list and selected reusable components.

c. Review data and process models (e.g., entity relationship and process hierarchy diagrams),

d. Confirm the decomposition of AIS into subsystems (if applicable), and

e. Approve the functional baseline.

The documents that are reviewed are: Requirements Specification, Requirements Traceability Matrix, and any changes to documents approved by the Technical Review Board during the Concept Phase. Requirements documents will be validated against the

System Boundary Agreement and the Project Management Plan and will be reviewed for completeness and consistency. See IT-212.2-04, Quality Assurance, for additional guidance in preparing review materials, and attending and conducting Detailed Level Requirements Review.

4.3 Business Transition Planning

Once the Concept of Operations has been accepted by the Program Sponsor, the Project Manager will work with the business area to plan how the organization will migrate to the desired business process. The Project Manager will use the Concept of Operations TSG, IT-212.2-11, as the guideline for designing and planning transition activities.

Special attention must be given to reducing any adverse impact that may result from the transition process.

4.3.1 Transition Activities

Transition activities cover all personnel, business process, budget, and organizational changes. Each transition activity is a required task and includes activities such as: revising policies, procedures, and job descriptions, providing training, establishing standard office formats, and providing necessary facilities and infrastructure to accommodate computer systems or work activities. In developing the transition activities, the Project Manager should coordinate with USPTO management to work with the unions to identify specific activities regarding labor management relations that must be implemented to provide a smooth transition to the new business processes. The accumulation of all transition activities will form the Business Transition Plan (refer to IT-212.3-05). All transition and change management activities will be documented and tracked in the Project Management Plan according to IT-212.2-01.

4.3.2 Preparing the Organization for Change

Special attention must be given to reducing any adverse impact that may result from the transition process. Project Managers should prepare their organization to effectively cope with change by building consensus among key personnel in affected groups. This can be accomplished by establishing more effective communications with internal and external customers, effectively managing labor relations through early and frequent communications, and by openly discussing anticipated changes with employees.

4.4 AIS Technical Architecture and Detailed Design

A technical architecture is a detailed design of the AIS hardware and software components, and their interrelationships. In the Detailed Analysis and Design Phase, the technical architecture for the AIS is captured in the Detailed Design Document and described in sufficient detail to guide the integration of applications and data to be developed in later life cycle phases as specified in the Detailed Design TSG, IT-212.4-12. The allocated baseline is established by mapping detailed requirements to the architectural elements identified in the high level architecture.

In the Detailed Analysis and Design Phase, the technical architecture for the AIS is described in sufficient detail to guide the integration of applications and data to be developed in later life cycle phases .

The detailed design must show the major types of processing platforms, how they interconnect, and the allocation of processing and storage resources to ensure that business requirements can be satisfied within system boundary constraints. An analysis of the architecture's capabilities must be conducted to determine performance and growth constraints in hardware, operating system software and utilities, and support software. All external system interfaces and internal subsystem interfaces must be identified and defined as specified in the Interface Design Definition, IT-212.3-14. The following policies are applicable to defining the technical architecture for this phase.

4.4.1 Use of Existing System Components or Commercial Off-The-Shelf (COTS) Products

The use of reusable components and/or COTS products, which comply with the USPTO Technical Reference Model, may significantly reduce the effort required to develop, test, and deploy the AIS, and should be a consideration in defining the AIS architecture. Design of new systems, subsystems, or components should be initiated only after a review of COTS

The use of reusable components and COTS products, which comply with the USPTO Technical Reference Model, may significantly reduce the effort required to develop, test, and deploy the AIS...

products and existing USPTO system components indicates that COTS or existing PTO system components can not be used or economically modified to satisfy functional requirements.

4.4.2 Design Characteristics

The Detailed Design must comply with the USPTO Technical Reference Model. The technical architecture will:

a. Define the hardware, software, and network components in which the AIS will operate,

b. Show how functional, data, and electronic records management requirements will be allocated among these components, and

c. Describe the means used to interconnect these components.

Characteristics of the detailed design specified during the Detailed Analysis and Design Phase should establish confidence that the system components, when integrated, will meet all functional, performance, and support requirements. The detailed design establishes a level of uniformity for further AIS design and development. Architectural limitations, such as the ability to handle changing user needs, increased performance, and upward compatibility to new technologies, must be determined, and if necessary, classified as project risks. The Detailed Design must:

a. Allow for maximum automated generation of application-specific code and databases using the CASE tool.

b. Allow for maximum reuse of existing system components.

c. Employ COTS software products wherever economically feasible.

d. Ensure that the application software can be processed on hardware and system software that is either currently available in the USPTO inventory or has been approved for acquisition and delivery in sufficient lead-time to allow for use during the test process of the Development Phase.

e. Provide for the collection of performance metrics.

f. Provide for including designer-added software capabilities for internal controls to facilitate functional and technical audits of the AIS.

g. Specify functional and technical requirements for integration of the AIS with other PTO business processes, as needed.

h. Handle sensitive information as specified in security related policies and requirements.

4.4.3 Prototyping

The use of prototyping is encouraged. Prototypes can be useful in refining requirements and may significantly enhance both user and developer understanding of requirements. Prototypes can also be used to validate portions of the technical architecture against the functional requirements, technical specifications, and may be used to obtain performance measures. In the Detailed Analysis and Design Phase, emphasis should be given to architectural prototypes that demonstrate the ability to integrate the preferred reusable components or COTS products into a coherent system that can satisfy functional, performance, and support requirements.

> *In the Detailed Analysis and Design Phase, emphasis should be given to architectural prototypes that demonstrate the ability to integrate the preferred reusable components or COTS products into a coherent system that can satisfy functional, performance, and support requirements.*

4.4.4 Peer Reviews

Peer reviews will be conducted on designated critical AIS projects to identify and remove defects from the products early and efficiently. Peer reviews can be particularly effective when used to review the work products and documentation developed during the Detailed Analysis and Design and Development phases of the life cycle. AIS or infrastructure project development documentation will be reviewed in accordance with the Quality Assurance TSG, IT-212.2-04. For designated AIS projects, reviews, inspections and walk-throughs will be scheduled, conducted, tracked, and the results reported in accordance with the project's Quality Assurance Plan.

4.5 Subsystem Identification, Definition and Management

4.5.1 Evolutionary Development and Incremental Delivery of Capabilities

The Project Manager and the System Development Manager are encouraged to follow an evolutionary development approach and divide up the AIS Project into several smaller components or subsystems. Based upon an analysis of the business processes, the Project Manager and System Development Manager should focus on providing end users with needed capabilities as early as practical. Typically each subsystem performs a unique function and supports an easily identifiable segment of the desired business process. Subsystem identification and definition occurs early in the Detailed Analysis and Design Phase.

Based upon an analysis of the business processes, the Project Manager and the System Development Manager should focus on providing end users with needed capabilities as early as practical.

Subsystems must be identified in the high level architecture and sufficiently documented to support adequate subsystem testing, integration, and integration testing. The Project Manager and the System Development Manager allocate requirements to subsystems based upon commonality of purpose in such a manner as to minimize the number of interactions that must occur between distinct subsystems. Interfaces between subsystems will be identified in terms of shared entities and functional services. Project management must update the Quality Assurance Plan to show the documents and reviews planned for each subsystem.

The Project Management and Business Transition Plans should be reviewed and updated to ensure that subsystem deployment is synchronized with changes in business practices and procedures. A Functional Baseline may be established at the end of the Detailed System Analysis Subphase and subsystem changes controlled in accordance with the Configuration Management TSG, IT-212.2-06.

4.5.2 Subsystem Project Management

The System Development Manager will designate a Lead Analyst for each subsystem to be developed. The Detailed Design Document and the Interface Design Definition will reflect the scope, requirements, performance measures, cost, and schedule for the system, including the subsystems. The individual subsystems will be controlled and coordinated within the boundaries established by the project System Boundary Agreement. See IT-212.2-12 and IT-212.3-14 for guidance on developing and documenting the Detailed Design Document and the Interface Design Definition, respectively.

4.6 COTS Detailed Analysis and Design Considerations

COTS software products seldom provide the functionality necessary to address all business requirements. System Development Managers will not modify the COTS product. USPTO unique requirements not provided by the COTS product will be satisfied through application program interfaces. Unless the COTS software firm fully supports USPTO unique modifications and makes them generally available to the public, the software package is no longer a COTS package. At this point there is a significant risk to the USPTO that the former COTS package may not perform as expected or be supported over time. Moreover, if the System Development Manager implements a modification in a COTS product, it may be very costly, if not impossible, to obtain vendor support in resolving software performance issues, even those apparently unrelated to the modification.

The System Development Manager must consider the time and skills needed to integrate COTS components into an AIS. Developers must specify, design, code, document, and test "in-house" software that will support COTS integration. When constructing COTS integration software, it may be necessary to verify COTS specifications and performance through unit testing or with prototypes. The System Development Manager must also keep in mind that new versions or COTS upgrades may alter the external interface to the COTS package. Software developers may find that it is necessary to design, integrate, and test integration software for new COTS releases to ensure compatibility with the existing AIS and other COTS components of the AIS. The System Architect will approve the selection of COTS software products.

4.7 Project Risk Management

During this phase the Project Manager and System Development Manager will continue to identify and evaluate risks to AIS project requirements, cost, and schedule. Issues related to managing AIS project requirements, creating AIS designs and supporting plans, and establishing realistic Subsystem Boundary Agreement conditions, contribute to project risks during this phase. Risks associated with an inability to quantify, verify, or test requirements can also begin to affect AIS project performance during this phase. The most significant risks during this phase, however, are typically risks that result from an inability to monitor or evaluate the effectiveness and timeliness of AIS analysis and design. Peer reviews can provide useful information used to identify risk classes, establish risk management criteria, and establish risk management measures associated with analysis and design activities. The risk management section of the Project

Management TSG (IT-212.2-01) provides additional guidance for managing AIS project risks.

4.8 AIS Security

During the Detailed Analysis and Design Phase project management will initiate preliminary steps to systematically identify and analyze AIS security requirements. The Project Manager should work closely with the security analysts in the Office of Information Systems Security (OISS) in analyzing security requirements. The AIS project team may apply information provided in the preliminary risk assessment to prototype security measures and safeguards. The System Development Manager may also use this information to develop back-up, contingency, and operational support plans. The Project Manager will advise the Program Sponsor, the CIO, the Systems Development Manager, and the OISS on matters of significant security threats.

The AIS project team may apply information provided in the preliminary risk assessment to prototype security measures and safeguards. Developers may use this information to enhance back-up, contingency, and operational support plans.

4.8.1 Security Analysis and Design

Both the Project Manager and the System Development Manager must work closely with USPTO security analysts to identify, analyze, and prioritize AIS security issues during this phase. With the assistance of AIS security specialists the AIS project team will determine what security features, assurances, and operational practices are appropriate to address these issues. In designing the AIS, the System Development Manager must incorporate these security requirements into the AIS design specifications. AIS security analysts will evaluate security requirements, designs, and supporting plans upon request and will advise project management, the Program Sponsor, CIO, or the Technical Review Board regarding areas of weakness or needed improvement.

4.8.2 Determining Security Requirements

Security requirements should be developed at the same time system requirements are defined. These security requirements can be expressed as technical features (e.g., log-in procedures or other access controls), assurances (e.g., background checks for system developers and users), or operational practices (e.g., awareness and training). The Project Manager, System Development Manager, OSAE, and USPTO security analysts must actively work together to ensure that the technical designs reflect the system's security needs. AIS security requirements, like other system requirements, are derived from a number of sources including law, policy, applicable standards and guidelines, functional needs of the system, risk assessment, and cost-benefit trade-off and are documented in the risk analysis.

4.8.3 Incorporating Security Requirements into Specifications

Security analysts will provide the Project Manager with reports that identify, estimate, and evaluate significant security issues, and, if requested, will research and recommend safeguards that address these issues. This analysis can result in voluminous amounts of information that must be validated, updated and organized into detailed security requirements and specifications.

During the development of AIS security specifications, it may become necessary for the Project Manager to re-examine initial risk assessments to ensure that all requirements are compatible and feasible to implement. The Project Manager must be able to determine that security features and practices will work correctly and effectively as early in the system life as possible. The Project Manager will brief the Program Sponsor, CIO, or Technical Review Board as recommended by the security analyst. Based upon the recommendations of the Project Manager, the Program Sponsor or the CIO may assign additional staff or allocate additional resources to ensure the development of that adequate AIS security specifications.

4.9 Logical Design Review

The products of the detailed requirements analysis, including the high level architecture and support plans must be reviewed by the Technical Review Board. The Logical Design Review will confirm that the business area logical model is sufficiently complete, correct, and stable to allow for the physical design to begin. Deficiencies identified in the logical model must be resolved, and changes generated by the review must be incorporated into the logical design as directed by the Technical Review Board. The High Level Architecture will be reviewed to verify its ability to satisfy the approved functional, data, and support requirements. Components of the logical model and other requirements shall be allocated to components of the technical architecture. Traceability shall be demonstrated to ensure that decisions concerning the high level architecture account for all allocated requirements. Issues governing the possibility of future change in the business or information technology infrastructure and the ability of the information and technical architectures to endure those changes shall be identified and appropriately addressed. This includes an analysis of the performance and growth requirements for the system throughout its planned operational use. Support plans will be validated against the Project Management Plan and will be reviewed for completeness and consistency. The support plans which are reviewed are: Test Plan, Training Plan, components of the Operational Support Plan including provisions for network and computer equipment. support, and any changes to plans approved by the Technical Review Board during the Concept Phase. The Logical Design Review (which may be conducted as one or more events) will be conducted in accordance with IT-212.2-04, Quality Assurance. The approved High Level Architecture and approved products of detailed requirements analysis shall be placed in a Logical Design (allocated) Baseline under configuration control.

The Logical Design Review will confirm that the business area logical model is sufficiently complete, correct, and stable to allow for the Development Phase to begin.

4.10 Technical Design Review

The Technical Design Review is conducted during the Detailed Analysis and Design Phase to evaluate the appropriateness of the technical design. This review verifies that the system conforms to the infrastructure baseline. The products of the Detailed Analysis and Design Phase, and updates to existing plans and specifications must be reviewed by the Technical Review Board. The Technical Design Review will confirm that the AIS or infrastructure system design is complete, correct, and ready for the Development Phase to begin. The Technical Design Review will be conducted in accordance with IT-212.2-04, Quality Assurance.

4.11 Analysis and Design Considerations

The overriding consideration when beginning to implement the final code and architecture for a system is to thoroughly understand the requirements and design. The following should be in place to begin development or existing problems/design holes will only be amplified down the road with project delays, unhappy users, and cost overruns.

a. Requirements should be known in detail. Functional requirements should be linked to the finished design. Detailed finalized screen formats, menu items, fields (mandatory and optional), and report layouts are necessary to proceed.
b. The database design should be complete. The physical design and its mapping to interfaces, screens fields and reports columns must be solid.
c. The mapping of legacy data to the new physical database should be established for all fields. Methods for handling rejected conversion data and illegal data values should be in place.
d. User access levels should be known. The functionality, data, and fields each user type is allowed to access should be detailed.
e. An estimate of frequency and size of all transactions, number of users, user screen use, report volumes should be created. This will ensure that the architecture and hardware products are sufficient to support required response times and data volumes.
f. Key Volume Indicators (KVI), process static reporting, management information requirements, maintenance hooks, and other enterprise-wide requirements should be addressed in this phase.
g. Design elements that are not defined because the requirements are not finalized due to technical risk elements that require prototyping should be identified in the Detailed Design Document and completed in the Development Phase.

DEVELOPMENT PHASE

5.1 Introduction

5.1.1 Purpose

During the Development Phase the Project Manager and the System Development Manager work closely together to:

a. Develop, integrate, and test the AIS,

b. Update and finalize plans to deploy the AIS, and

c. Complete business transition planning and initiate business transition activities.

During the Development Phase the Project Manager and the System Development Manager work closely together to develop, assemble, integrate, and test the AIS, and to update and finalize the plans for the deploying the AIS.

5.1.2 Overview

The Development Phase is divided into two stages: Construction and Production Readiness. In the Construction Stage, the System Development Manager ensures that all AIS subsystems, modules, and components are fully documented, have been coded and tested, and that identified discrepancies have been corrected. The Construction Stage is completed when the Technical Review Board provides approval at Test Readiness Review. Earlier test results are reviewed and operational support arrangements are finalized during the Production Readiness Stage. The Production Readiness Stage ends with successful completion of the Production Readiness Review. This review affirms that Acceptance Testing has been successfully completed and that the AIS is suitable for production use.

5.1.3 Tasks

The tasks to be completed during the Development Phase are:

a. Allocate resources to support the current project plan.

b. Complete business transition planning, and begin business transition activities.

c. Perform component provisioning of reusable components.

d. Code software that is not commercial off-the-shelf (COTS) and is not generated by the CASE tools.

e. Perform module construction and application assembly of reusable components, and complete integration.

f. Complete acquiring equipment and approved COTS software for the AIS.

g. Complete AIS support documentation, including training.

h. Perform system testing activities to include unit and integration testing, performance, and stress testing.

i. Update the Configuration Management Plan.

j. Perform a Configuration Management Build.

k. Update the Economic Analysis.

l. Update the Project Management, AIS Development, and Quality Assurance Plans.

m. Update support plans.

n. Develop the Production Installation and Data Conversion Plans.

o. Update the technical architecture with details of the physical implementation.

p. Perform Formal Qualification Testing[1] (FQT) and Beta Testing[2].

q. Obtain approval to install the AIS into work areas.

r. Software development environment planning activities should be defined and submitted to OSDM/SDI.

5.1.4 Activities and Documentation

Development Phase activities and documentation requirements as summarized in the following table must conform to the indicated Technical Standard and Guidelines or other standards as noted. Work products included in the Product Baselines are identified under

[1] *Formal Qualification Testing (FQT)* exercises the entire AIS to independently confirm and extend integration testing results in an environment that more closely duplicates the production environment. OSPA will test all AIS requirements that can reasonably be tested. These requirements are identified in the current AIS requirements traceability matrix. See 5.4.6 below.

[2] Beta testing may be tailored in or out of the life cycle. End users perform *Beta Testing* in an ad hoc manner to confirm that the system will provide the expected functionality before placing the system into full service. This testing will simulate the production environment as closely as is reasonably possible. See 5.4.7 and 5.4.8 below.

the "Baseline" heading in Table 5.1.4. Published standards and guidelines may be augmented by tailoring and documented in the Quality Assurance Plan.

Work Product	TSG / Standard	Who's Responsible	Must Create	Should Update	Must Update	Base - line	Must Complete
Business Case		Program Sponsor, Project Manager				X	
Project Management Plan and supporting baseline project schedules	IT-212.2-01	Project Manager, System Development Manager			X		
AIS Project Quality Assurance Plan	IT-212.2-04	Office of System Product Assurance		X			
Data Management Plan	IT-212.2-05	Office of Data Management		X			X
Data Conversion Plan	IT-212.2-05	System Development Manager	X				X
AIS Configuration Management Plan	IT-212.2-06	Office of System Product Assurance		X			X
Concept of Operations	IT-212.2-11	Program Sponsor, Project Manager			X		X
Detailed Design	IT-212.2-12	System Development Manager			X		X
Economic Analysis	IT-212.2-13	Project Manager, System Development Manager			X		X
Business Transition Plan	IT-212.3-05	Program Sponsor, Project Manager		X			X
Requirements Specification	IT-212.3-10	System Development Manager		X		X	X
Test Plan and Materials	IT-212.3-01	Office of System Product Assurance			X	X	X
Test Specifications and Procedures	IT-212.3-01	Office of System Product Assurance	X				X
Training Plan and Materials	IT-212.3-02	System Development Manager			X	X	
Requirements Traceability Matrix	IT-212.3-11	Office of System Product Assurance		X			

Table 5.1.4 Development Phase Activities and Documentation Requirements

Work Product	TSG / Standard	Who's Responsible	Must Create	Should Update	Must Update	Base - line	Must Complete
Users Manual and/or Guide	IT-212.4-13	System Development Manager	X				X
Infrastructure Disaster Recovery Plan	IT-212.2-08	Office of System Network Management	X				X
Programmer Maintenance Manual	IT-212.4-15	System Development Manager	X				X
CM Build Instructions with Version Description Document	IT-212.2-06	System Development Manager	X				X
Production Installation Plan	IT-212.5-01 01	System Development Manager	X				X
Operational Support Plan	IT-212.5-01	System Development Manager					X

Table 5.1.4 Development Phase Activities and Documentation Requirements (Concluded)

5.2 System Development

5.2.1 Software Development and Construction

Application code, databases, database conversion software, interfaces, and code to integrate COTS products into the AIS are constructed during the Development Phase. The following points apply to software development.

Reviews, inspections and walk-throughs will be scheduled, conducted, tracked, and the results reported in accordance with the project's Quality Assurance Plan.

a. To improve software documentation and maintainability, whenever possible, changes to AIS application code will be implemented using USPTO standard CASE tool procedures. For later enhancement or maintenance, source code that had been automatically generated will be regenerated and not manually modified.

b. All code will be designed, documented, and developed using modern software development concepts, tools, and techniques. The supporting documentation will be reviewed by the Office of System Product Assurance for accuracy, efficiency, completeness, and ease of use.

c. Developers will thoroughly document and test all software that performs automated conversion of data from existing to new databases. The supporting documentation will be reviewed by the Office of System Product Assurance for accuracy, efficiency, completeness, and ease of use.

d. Using the component specification, the component provisioning task delivers an executing and tested implementation of the component. Each component implementation is designed, coded, and tested. For each reusable CASE component:

   - The component is specified in the CASE encyclopedia.
   - The component implementation model is constructed to meet the component specification model.
   - The component executable is generated from the component implementation model.

e. The component publishing task places the component specification in a USPTO Enterprise Repository component catalog that should be browsed for review in future projects. Publishing produces an installation package to deploy the component into an AIS development environment. The entire model specification, including the data and behavior of the component, should be published for browsing.

f. TRM designated programming languages will be used in all USPTO multi-user applications. Nonstandard, high-order programming languages, as are commonly associated with COTS products, may be used for single user applications or where it can be shown to be more cost-effective for multi-user applications.

g. To help ensure code portability and scalability, developers will not use vendor-unique extensions unless it can be shown to be cost-effective over the life of the application. Waiver requests to use vendor-unique extensions must be submitted to the Technical Review Board for approval. Waivers are not required to use:

- COTS software packages and advanced software technology that is not modified or maintained by the USPTO and can operate on the USPTO information technology infrastructure.
- Programming languages that require installation of vendor-provided updates to COTS software. Use of such languages shall be restricted to implementing the vendor updates.

5.2.2 Integration

Hardware, software (including COTS software), and documentation components which have been individually tested are assembled into functional subsystems and systems in accordance with the project's quality assurance and configuration management plans. Application components must be integrated. Either part or all of an entire application may be built by assembling components. The component verification activity includes installation of components into the environment where they will reside when assembled into an application to verify that installation procedures work. The System Development Manager will complete and update all system design and support documentation in accordance with the applicable Technical Standards and Guidelines. Integration may be performed iteratively with increasingly larger and more complex combinations of components. The steps in which integration will occur shall be documented in the project's AIS project management and test plans. Integration is completed when the entire AIS has been assembled, integration level testing has been performed, and integration test results have been approved by the Technical Review Board at Test Readiness Review.

5.3 Testing and Reviews

Unit, integration, and independent acceptance testing activities are performed during the Development Phase. Unit and integration testing are performed under the direction of the Project Manager and System Development Manager. Independent acceptance testing is performed independently from the developing organization and is coordinated by the Office of System Product Assurance. The independent acceptance testing activities performed during the Development Phase are Formal Qualification Testing and Beta Testing. Defects uncovered by acceptance testing may lead to changes in the work products created in the Concept, Detailed Analysis and Design, and Development Phases. The technical standards and guidelines for those phases apply, as needed, during the Development Phase. As much as possible, acceptance testing will be performed in a test environment that duplicates the production environment. The Technical Review Board reviews the results of each test. Additional information on testing is provided in the Testing TSG, IT-212.3-01.

5.3.1 Design Characteristics

Each program module will be separately tested and verified to ensure that all applicable business requirements and module interface specifications are addressed, and that all unit products conform to design specifications. Unit testing should verify that every logical path through the pseudo-code (or detailed module description) is implemented and functions as designed, and that no unit level code is accepted that is not designed and documented). All errors and discrepancies noted will be corrected.

> *Each program module will be separately tested and verified to ensure that all applicable business requirements and module interface specifications are addressed, and that all unit products conform to design specifications.*

5.3.2 Independent Security Testing

The Office of System Product Assurance and the Office of Information Systems Security will conduct independent system security testing during the Development Phase. System security testing includes both the testing of the particular AIS components, including both purchased and “in-house developed” components, and the testing of the entire AIS. Security management, physical facilities, personnel, procedures, the use of commercial or COTS products, the use of OCIO services (such as PTOnet services), and contingency plans are examples of security areas that affect the entire AIS. Because Project Managers or System Development Managers usually specify or determine requirements relating to these security areas before or after the Development Phase, additional security testing is usually necessary throughout the life of the system. The Operational Support TSG, IT-

212.5-01, and the Testing TSG, IT-212.3-01, provide additional information about testing AIS security requirements.

5.3.3 Peer Reviews

Peer reviews will be conducted on designated critical AIS projects to identify and remove defects from the products early and efficiently. Peer reviews can be particularly effective when used to review the work products and documentation developed during the Detailed Analysis and Design and Development phases of the life cycle. AIS or infrastructure project development documentation will be reviewed in accordance with the Quality Assurance TSG, IT-212.2-04. For designated AIS projects, reviews, inspections and walk-throughs will be scheduled, conducted, tracked, and the results reported in accordance with the project's Quality Assurance Plan.

5.3.4 Test Readiness Review

This review is conducted at the end of the Development Phase to determine whether unit and integration testing has been conducted in accordance with the test procedures and that the tests are complete. The Project Manager reviews and approves test procedures, specifications, test procedure modifications (i.e., redlines), and the results of all integration tests before requesting Technical Review Board review and approval of integration testing at Test Readiness Review. A version of the Developmental Configuration is placed under formal configuration management after Test Readiness Review and is used for acceptance testing.

5.3.5 COTS Acceptance Testing

Acceptance testing of COTS products will be performed and all problems and defects will be corrected in accordance with the terms of the contract or other purchase agreement. Unit level testing of COTS products may not be required in circumstances where acceptance testing of the COTS product has been performed and documented. COTS acceptance testing procedures and specifications, and all results of COTS acceptance testing will be reviewed, and if accepted by the Project Manager, will forwarded to the Technical Review Board for review and approval at Test Readiness Review. The Office of System Product Assurance may perform independent testing of COTS products.

5.3.6 Integration Testing

Integration testing verifies the interoperability of AIS modules, components, and subsystems, up to the complete AIS, to ensure that all functional and technical objectives are achieved. Typically, test data must be specifically designed and developed to ensure full coverage of all requirements, and to ensure that all procedural and control options in the AIS code are tested. When possible, actual data should also be used in integration testing to ensure consistency between AIS specifications and the desired business process. The results of all integration tests must be recorded. Test Procedures are corrected by redlining the test procedures document to show changes.

5.3.7 Formal Qualification Testing (FQT)

Formal Qualification Testing is an independent acceptance testing activity performed on an approved Configuration Management Build by the Office of System Product Assurance. During this testing activity all AIS functional capabilities, including security measures, are independently exercised to verify that the AIS meets all functional and security requirements. Formal Qualification Testing is performed against the requirements identified in the project's Requirements Traceability Matrix in accordance with the redlined test specifications and test procedures developed during integration testing.

5.3.8 Beta Readiness Review

When a Beta Readiness Review is conducted, it verifies that formal testing is complete and that the system is ready to be tested by selected users, including employee union representatives. The Office of System Product Assurance will forward the results of Formal Qualification Testing to the Technical Review Board for review at the Beta Readiness Review. This review will be conducted in accordance with the project's Quality Assurance Plan and test plans. The AIS will not be installed in production work areas or operational facilities, or connected to production systems without the concurrence of the Project Manager.

5.3.9 Beta Testing

During Beta Testing selected users test routine features of the AIS to verify that the AIS performs as expected. Beta testing exercises the entire system as it is commonly used, rather than testing it extensively against formal statements of requirements. In preparation, the Beta testers will receive training on the AIS using the training material delivered with the AIS. The Project Manager selects test participants and establishes the schedule for Beta Testing.

5.4 Project Risk Management

The Project Manager will continue to evaluate risks to AIS project requirements, cost, and schedule. The most common risks encountered during the Development Phase relate to events that may prevent full development or implementation of AIS project requirements. Security requirements and controls, if not previously addressed, will impose significant project risk during the Development Phase. This is due to the potential cost and complexity necessary to retrofit these requirements and designs into the AIS late in the life cycle. Significant risks will also result if review and approval of designs and supporting plans, development tools, development skills, appropriate unit and integration testing, or specification, installation and testing of security controls are inadequate. AIS project managers must also evaluate the risks associated with recent changes and upgrades to the hardware configuration, operating system and system utilities, software development tools, and AIS COTS components. The Project Manager will advise the Program Sponsor and the CIO on matters of significant risk. The Project Manager will also coordinate risk management activities with key managers and analysts based upon their ability to control risk. The Project Management TSG, IT-212.2-01, provides additional guidance on managing risk.

5.4.1 Project Risk Assessment

The Project Manager and the System Development Manager will continue to analyze the existing project situation to identify, analyze, and mitigate significant AIS project risks. These managers will focus on ensuring the full implementation of AIS project requirements. AIS project management will also focus on providing appropriate review and approval of designs and supporting plans, and completing appropriate unit and integration testing that includes testing of security requirements. The Project Manager must also provide appropriate review and approval for changes in hardware, software, development tools, and COTS components. The Project Manager and the System Development Manager will ensure the complete documentation of information and activities that identify, estimate, and evaluate significant risks.

5.4.2 Project Risk Review and Mitigation

Risk assessment findings will be presented to the Program Sponsor, Technical Review Board, or the CIO, as necessary. These presentations will reaffirm the significance of risks and will solicit management support for addressing significant risks. Based upon the recommendations of the Project Manager, the Program Sponsor or the CIO may assign additional staff or allocate additional resources to control significant risks.

5.5 AIS and COTS Security

Security activities for an AIS may include:

a. developing AIS security aspects,

b. monitoring the development process itself for security problems,

c. responding to requirements changes from a security perspective,

d. monitoring security risks.

Security risks that may arise during the Development Phase include risks associated with code intentionally designed to defeat security measures and disguised as useful code, incorrect code, poorly functioning development tools, manipulation of code, and malicious insiders.

Security activities for COTS software may include monitoring to ensure that security is part of market surveys, contract solicitation documents, and evaluation of proposed systems. Many systems use a combination of "in-house" development and COTS acquisition. In this case all the security activities discussed above are applicable.

As the AIS is built, choices are made about the system, which can impact security including: selection of specific COTS products, AIS architecture, and, AIS site or hardware selection. In addition, security activities such as contingency planning, security awareness training, and security documentation must be conducted. The Operational Support TSG, IT-212.5-01 provides additional information regarding the operational aspects of AIS security. Security, like all requirements, must be anticipated from the beginning of the Initiation Phase.

5.6 Business Transition Planning

Business Transition Planning, which began during the Detailed Analysis and Design Phase, continues through the Development Phase following the guidance contained in the Business Transition Planning TSG, IT-212.3-05. All significant changes to the business process made during the Development Phase must be reviewed by the System Development Manager, and

Transition activities should be tested during the Development Phase to ensure that all personnel, business process, and organizational changes can be implemented with minimum disruption to ongoing production.

reviewed and approved by the Project Manager. The Program Sponsor and Project Manager should coordinate significant business process changes with the employee union representatives.

5.6.1 Transition Activities

Transition activities should be reviewed and evaluated during the Development Phase to ensure that all personnel, business process, and organizational changes can be implemented with minimum disruption to ongoing production. Where feasible, interviews and surveys should be conducted to identify issues and determine the level of acceptance to changes in policies, procedures, and job descriptions. Additional changes in the Business Transition Plan may be necessary based upon feedback collected though this process. Moreover, specific presentations and specialized training sessions may be needed to further emphasize the intended goals and benefits of the process improvement activity, including AIS support. All transition and change management activities will be documented and tracked in the Project Management Plan according to IT-212.02-01. The Project Manager may brief the Technical Review Board on the expected impact the deployed AIS will have on their organization at Test Readiness Review.

5.6.2 Preparing the Organization for Change

End user involvement in the specification, design, development, and testing of transition activities is absolutely essential to promote broad-based process ownership and acceptance. During the Development Phase, end users and the employee union representatives should be heavily involved in transition activities which require pilot testing (e.g., workflow redesign, team-oriented examination) and should play a major role in reporting the results of pilot tests. Moreover, end users should be involved in updating the desired business process and in planning AIS deployment throughout the organization. Where feasible, end users should take the lead in validating revised policies and procedures, new forms and formats, job aids, and performance measures.

5.7 Production Readiness Review

At the Production Readiness Review, the TRB will confirm that the AIS is complete, correct, fully tested, and ready for the Deployment Phase to begin.

The products of the Development Phase, and updates to existing plans and specifications must be reviewed by the Technical Review Board. The Production Readiness Review will confirm that the AIS is complete, correct, fully tested, and ready for the Deployment Phase to begin. This review establishes the product and operational baselines and confirms that appropriate operational and maintenance support is available. The Product Baseline consists of the documentation describing all the necessary functional and physical characteristics of the elements that compose the system and the actual equipment and software. The Technical Review Board will confirm that the installation of the AIS into the production environment will have no adverse impact on other AISs or the PTO information technology infrastructure.

Deficiencies identified in unit, integration, Formal Qualification, and Beta Testing must be resolved, and changes generated by the review must be incorporated into the appropriate work products as directed by the Technical Review Board. Based upon a finding that the AIS is suitable for production use, the Technical Review Board will recommend to the Program Sponsor and CIO to the deploy the AIS in accordance with the Production Installation Plan.

DEPLOYMENT PHASE

6.1 Introduction

6.1.1 Purpose

During the Deployment Phase the Project Manager accepts the AIS or infrastructure system into production for trial operation. The System Development Manager works together with the Project Manager to ensure that:

As the new AIS or infrastructure system is introduced into the workplace, it is critically important that the Project Manager and the System Development Manager implement the Deployment Plan in a coordinated manner.

a. The AIS or infrastructure system is installed as planned and specified,

b. Users are trained,

c. End users and supporting organizations are prepared to accept the system.

For these goals to be met, it is vitally important that the Project Manager and the System Development Manager carefully plan for the eventual deployment of the system including needed staffing, training, as well as anticipated policy and procedure changes. Moreover, once this planning has been completed it is critically important that the Project Manager and the System Development Manager implement these plans in a coordinated manner as the new AIS or infrastructure system is introduced into the workplace.

6.1.2 Overview

The AIS or infrastructure system is installed to support the intended business functions. Performance objectives are identified, agreed to, and recorded in a Service Level Agreement before going into operation. The Project Manager decides when deployment to the workforce is to begin and determines the general deployment schedule and approach. From a technical perspective this phase is concerned with installation, operational assessment, and independent acceptance of the AIS or infrastructure system. Users, operational support staff and testers from outside the developing organization must

Users, operational support staff, and testers from outside the developing organization must be involved in accepting the AIS or infrastructure system.

be involved in accepting the AIS or infrastructure system. From the business point of view, this phase is concerned with ensuring that the customer organization is fully trained and prepared to use the new or modified AIS or infrastructure system.

6.1.3 Tasks

The tasks to be performed during this phase are:

a. Ensure that deployment, operational support, and maintenance resources are adequate.

b. Train user and information technology support personnel.

c. Prepare the sites where the AIS or infrastructure system will be used and operated.

d. Install the system at sites designated by the Project Manager.

e. Complete all necessary data conversion.

f. Ensure that all documentation and procedures are fully developed and tested.

g. Conduct periodic Functional and Physical Configuration Audits.

h. Conduct AIS or infrastructure system security review.

i. Identify AIS or infrastructure system performance objectives in a Service Level Agreement contained in the OSP.

j. Ensure that adequate production and maintenance procedures are in place.

6.2 Production Installation

After the Technical Review board grants acceptance or conditional acceptance of the system at a Production Readiness Review, the site is prepared and the AIS or infrastructure system is installed in the production environment in accordance with the project's Production Installation Plan and the Project Management Plan. Production databases are converted in accordance with the project's Data Conversion Plan. Project managers must ensure that supplies are available, technical manuals or documents that may be needed for installation have been distributed, and that computer resources are available to support the production installation.

6.3 Configuration Audits

Functional and Physical Configuration audits are typically discussed under the topic of "acceptance" at this point in the life cycle. In the past this has contributed to some confusion regarding the distinction, if any, between "tests" and "audits". In some cases, such as in the distinction between a Formal Qualification Test and a Functional Configuration Audit, this difference can be very difficult to grasp without some background information.

The key difference between "tests" and "configuration audits" can be found in the intended purpose of the activity. Tests are conducted to verify that the AIS or some component of the AIS is fit for further development, integration, or use in terms of functionality, supportability, and maintainability. Configuration audits are conducted to verify that the AIS, or components of the AIS are fully and accurately represented, recorded, and managed within the configuration management system to a degree sufficient to ensure that specific requirements can be identified for all work products and configuration items (i.e., traceability). Results from earlier testing activities can be used to verify that work products and configuration items comply with requirements, and may provide part of the input to subsequent audits.

There are two types of audits that may be performed by the Office of System Product Assurance: Functional Audits and Physical Audits. Functional and Physical Audits may be conducted for an entire AIS or may be conducted incrementally on components of an AIS. When conducted together for an entire AIS, Functional and Physical Configuration Audits together establish the "Product Baseline". Both audit types are discussed below and detailed discussions of each are provided in the Configuration Management TSG, IT-212.2-06.

All contractor produced AIS components will be officially received by the Office of Acquisition Management and placed under configuration management control. Task Order Managers may also specify that contractors directly transfer electronically produced work products and configuration items into the configuration management system. Functional and Physical Configuration Management Audits will be conducted on AIS components once under configuration management control. The entire AIS will also be audited periodically following AIS integration, to verify that the complete AIS is fully and accurately represented, recorded, and managed within the configuration management system.

Both independent acceptance testing and independent audits are performed by the Office of System Product Assurance. The Office of System Product Assurance will not evaluate, test, audit, or recommend acceptance of any contractor produced AIS or AIS component that has not been officially received by the Office of Acquisitions

Management. The Office of System Product Assurance may not evaluate, test, audit, or recommend acceptance of any AIS or AIS component that does not reside in the standard USPTO configuration management tool.

6.3.1 Functional Configuration Audits

A Functional Configuration Audit is a formal examination of functional characteristics (e.g., performance, behavior, content) of a configuration item (e.g., AIS, subsystem, module, design document), to verify that the item has achieved the requirements specified in its documentation (e.g., system boundary, requirements specification, task statements, user manuals, contractor proposals). While these audits are typically performed at the end of the Development Phase to "certify" that all faults identified during Formal Qualification Testing have been resolved, these audits can also be conducted before acceptance testing to demonstrate that AIS software is sufficiently complete for acceptance testing to begin. Functional Configuration Audits are performed by the Office of System Product Assurance with the support of the Project Manager. Guidance on Functional Configuration Audits is provided in the Configuration Management TSG, IT-212.2-06.

6.3.2 Physical Configuration Audits

A Physical Configuration Audit is a formal examination of the existing configuration item (e.g., AIS, subsystem, product, deliverable, document, source code) to verify that:

a. requirements, specifications, and standards applied in producing the configuration item have been addressed, and

b. all features delivered can be traced though the development process and through technical requirements back to a specific set functional requirements.

The Office of System Product Assurance performs Physical Configuration Audits with the support of the Project Manager and System Development Manager. Guidance on Physical Configuration Audits is provided in the Configuration Management TSG, IT-212.2-06.

6.4 AIS or Infrastructure System Security (Accreditation)

Security measures and controls are activated and verified immediately before the beginning of the Deployment Phase. While this may seem obvious, this activity is frequently overlooked. Commercial software, COTS products, and custom-developed systems frequently arrive with their security features disabled. These features must be enabled and configured, and for many systems this is a complex task requiring significant skills. Another critical security activity, accreditation, occurs between the end of the Development Phase and the end of the Deployment Phase.

System security accreditation is the *formal authorization* by the CIO and the Program Sponsor for system operation that contains an *explicit acceptance of risk.* It is usually supported by a review of the AIS or infrastructure system, such as an Operational Assessment, and includes management, operation, and technical controls. This review *may* include a detailed technical evaluation (such as a Federal Information Processing Standards 102 certification, particularly for complex, mission critical, or high-risk systems), security evaluation, security risk assessment, audit, or other such review. If the AIS or infrastructure system is being enhanced or upgraded, it is important that the accreditation cover the entire AIS or infrastructure system and not be restricted to only the new addition.

Accreditation is a form of quality control. This control compels all USPTO managers associated with, or impacted by the project to work together to find the most appropriate security approach for the organization, given technical constraints, operational constraints, and business requirements. This process obliges these managers to make critical decisions regarding the adequacy of security safeguards. A decision based upon reliable information about the effectiveness of technical and non-technical safeguards and the associated risks is more likely to be a sound decision.

After deciding on the acceptability of security safeguards and associated risks, the CIO and the Program Sponsor should issue a formal accreditation statement. While most security defects will not be severe enough to prevent the AIS or infrastructure system from being placed into service, these defects may require some restrictions (e.g., restrictions on web or dial-in access, or connections to other organizations). In some cases, the CIO and the Program Sponsor may grant an interim accreditation allowing the system to operate, and requiring a review at the end of the Deployment Phase, presumably after the security defects have been corrected.

6.5 Business Transition

During the Deployment Phase, the Project Manager will coordinate AIS or infrastructure system installation, testing, and user training with business training in new processes, procedures, skill sets, workflows, job descriptions, and organizational structures. The status of this activity will be monitored and updated in the Project Management Plan as specified in the Project Management TSG, IT-212.02-01.

The Project Manager should focus on reducing all adverse impacts that the new AIS or infrastructure system might have on the organization. Successful achievement of project goals and objectives can only be accomplished with the full cooperation and support of the user community.

6.6 Training

The Project Manager and the System Development Manager will work with the business area training representative to coordinate training and implementation activities. Training on the use of the new or modified AIS or infrastructure system will use current training materials updated by Beta Testing. Training should include hands-on use of the AIS or infrastructure system in a "production-like" environment. The Project Manager, with the assistance of the business area training representative, the Patent Academy or the Workforce Effectiveness Division, shall train functional users and managers in the use of new business processes and procedures.

6.7 Transfer of System Management Responsibility

Upon completion of the Deployment Phase, the Program Sponsor transfers responsibility for management of the AIS or infrastructure system from the Project Manager to the Production Manager, and the CIO transfers responsibility for information technology support from the System Development Manager to the System Maintenance Manager. In some cases, to conserve resources and preserve business area and AIS or infrastructure system expertise, these personnel assignments may be nothing more than a change in title, or the addition of a title to current managers. The Production Manager should begin planning, as needed, for the first User Feedback Meeting to ensure that business needs continue to be addressed once the AIS or infrastructure system is in full production.

CONCEPT PHASE

3.1 Introduction

3.1.1 Purpose

The Concept Phase will determine whether an acceptable and cost-effective approach can be found to address the business need with high confidence that technology can support that approach. The purposes of this phase are to:

The Concept Phase will determine whether an acceptable and cost-effective approach can be found to address the business need with high confidence that technology can support that approach.

a. Establish system boundaries, identify goals, objectives, critical success factors, and performance measures,

b. Evaluate costs and benefits of alternative approaches to satisfy the basic functional requirements,

c. Assess project, technical, and business risks,

d. Identify and initiate risk mitigation actions,

e. Identify system interfaces,

f. Identify basic high level requirements to satisfy the business need,

g. Develop high level architecture, process models, data models, and a Concept of Operations[1], and

h. Identify high level electronic records management requirements.

[1] The Concept of Operations is prepared by the Project Manager and summarizes business structure, policies, procedures, and anticipated changes to the business organization. This document describes how the business area organization is currently structured, how it currently performs work, and how this organization may be structured in the future. The Concept of Operations also describes what new processes will be used to perform work in the future, and compares business process alternatives in terms of impact and risk to the organization.

For all AIS projects designated as mission critical, the Program Sponsor must approve high level requirements defined in the Requirements Specification[2] validating that the high level requirements provided therein are complete before a High Level Requirements Review can be conducted. This phase is completed upon approval of the high level requirements by the Technical Review Board at the High Level Requirements Review, and when the Program Sponsor and the CIO agree to the system boundary.

3.1.2 Overview

Following approval of the Business Case, the Concept Phase begins when the Project Manager appoints the project team[3] and the CIO appoints a System Development Manager. The Program Sponsor, with the assistance of the Project Manager and the System Development Manager, evaluates realistic approaches that address the Business Case and determines which approach will be implemented. This may involve making several trade-off decisions such as the decision to use COTS software products as opposed to developing custom software or reusing software components, or the decision to use an incremental delivery versus a complete, one-time deployment.

Project Managers and System Development Managers must work with the Office of System Product Assurance to tailor their life cycle processes to the specific needs of their AIS project.

Unnecessary and significant costs will be incurred if too much or too little effort is expended in planning, documenting, or reviewing an AIS project. A key decision that must be made during the Concept Phase is determining the appropriate level of effort for these activities given the scope, complexity and importance of the AIS under consideration. Project Managers and System Development Managers must develop the project tailoring and the System Development Manager coordinates with the Office of System Product Assurance during this phase to tailor their life cycle processes to the specific needs of their AIS project. These tailoring decisions will be reflected in the Concept Brief, the Project Management Plan, and in the Quality Assurance Plan. The AIS Life Cycle Process Tailoring TSG, IT-212.2-03, provides guidance for LCM tailoring. The Project Manager must ensure that the Project Management, Quality Assurance, Data Management, Operational Support, Test Plans,

[2] The Requirements Specification is organized into high level and detailed level requirements. Part 1 of the Requirements Specification (Sections 1, 2, 3.2, 3.2.1, 3.2.2, 3.3, and 3.3.1) documents the high level requirements and Part 2 (the remaining sections of the specification), documents the detailed level requirements.

[3] The project team is responsible for assisting the Project Manager in identifying detailed business requirements, and addressing end-user issues regarding planning, requirements validation, training, logistics, facilities, and end-user acceptance testing.

and the Detailed Design all reflect appropriate levels of security operations and administration.

Depending upon AIS size, scope, complexity, and risk, there may be as many as ten plans and documents initiated during the Concept Phase. Of these, only eight, the System Boundary Agreement (containing the statement of requirements), the Project Management Plan, the Configuration Management Plan, Data Management Plan, the Quality Assurance Plan, the High Level Architecture, Requirements Specification, and the Concept of Operations are absolutely required for all AIS development projects. These are the only Concept Phase documents that must be completed or have a baseline established before the beginning of the Detailed Analysis and Design Phase. An Economic Analysis is required for all AIS projects that are designated as mission critical. A Security Plan is required if the system processes sensitive data. The Program Sponsor, in signing the Requirements Specification, Part 1 validates that the high level business requirements are complete. In approving the Requirements Specification, Part 1, the Technical Review Board, with the assistance of the Office of System Product Assurance, verifies that the high level business requirements provided in the Requirements Specification, Part 1 are clearly expressed.

The Project Manager, the System Development Manager, and the System Architect should work together during this phase to estimate the extent to which COTS products will be used in meeting functional requirements. If significant use of COTS programming features is anticipated, then the System Development Manager must ensure that appropriate design, operation, testing, and maintenance documentation to adequately support the development of this code is provided for in the Project Management Plan. The System Development Manager will ensure that requirements, design, development, operation, and testing reviews necessary to adequately support the development of this code are conducted. The Office of System Product Assurance will ensure that these reviews and documents are specified in the Concept Brief and the Quality Assurance Plan.

During the Concept Phase, the Project Manager and the System Development Manager should also initiate discussions with the Office of Acquisition Management to plan for acquisition and contractor support to the AIS project.

3.1.3 Tasks

The primary tasks performed during the Concept Phase are as follows:

Many of these tasks can be performed more effectively with the aid of prototyping. Construction of executable prototypes is encouraged to confirm requirements or to evaluate technology needed to support the business process.

a. Update the business case,

b. Establish the system boundary,

c. Begin project planning and develop the Project Management Plan,

d. Develop the Concept of Operations,

e. Determine functional requirements and informational needs,

f. Develop the Requirements Specification, Part 1,

g. Develop the Quality Assurance Plan,

h. Develop the Configuration Management Plan,

i. Investigate alternative business processes and procedures,

j. Consider data management,

k. Identify electronic records management requirements,

l. Perform an economic analysis of alternatives,

m. Select the most cost-effective alternative,

n. Identify, estimate and allocate resources to support project plans and major activities,

o. Determine the level of contractor support needed for each major project activity,

p. Analyze project risk and initiate risk mitigation activities,

q. Define the High Level Architecture[4], and

[4] A High Level Architecture (HLA) defines the integration of business processes, data models, application software, and common information technology infrastructure components. The AIS High Level Architecture is a refinement of the Concept of Operations that symbolically describes the business functions, activities, and information flows that the AIS will provide or support. The HLA also describes the implementation of the AIS within the operational environment by providing textual and graphical descriptions of AIS hardware, software, and network components, and by illustrating the interconnections between these components. The HLA is refined during the Detailed Analysis and Design Phase and is the basis for preparing the Detailed Design. Additional information regarding technical architecture can be found in the Technical Architecture TSG (IT-212.2-12).

r. Plan acquisition needs.

Many of these tasks can be performed more effectively with the aid of prototyping. Construction of executable prototypes is encouraged to confirm requirements, manage risks, or to evaluate technology needed to support the business process. Prototypes must conform to the USPTO Technical Reference Model.

3.1.4 Activities and Documentation

Concept Phase activities and documentation requirements as summarized in the following table must conform to the indicated Technical Standard and Guidelines or other standards as noted. The Technical Review Board establishes the System Boundary Baseline during this phase. Section 3.3 of this document and the Configuration Management TSG, IT-212.2-06, provide additional information about the System Boundary. Published standards and guidelines may be augmented with Tailoring Agreements.

Work Product	TSG / Standard	Who's Responsible	Must Create	May Create	Should Update	Must Update	Must Complete
Business Case		Program Sponsor, Project Manager				X	
Project Management Plan	IT-212.2-01	Project Manager, SDM	X				
AIS Project Quality Assurance Plan	IT-212.2-04	Office of System Product Assurance	X				X
Data Management Plan	IT-212.2-05	Office of Data Management		X			
AIS Configuration Management Plan	IT-212.2-06	Office of System Product Assurance	X				
System Boundary Agreement	IT-212.2-10	Project Manager, System Development Manager	X				
Requirements Specification, Part 1		System Development Manager	X				
Concept of Operations	IT-212.2-11	Program Sponsor, Project Manager	X				
High Level Architecture	IT-212.2-12	Office of System Architecture & Engineering	X				X
Economic Analysis[1]	IT-212.2-13	Project Manager, System Development Manager	X[1]				X[1]
AIS Security Plan (If sensitive data)	IT-212.2-08	Project Manager, System Development Manager	X				
NOTE 1: Required for AIS Projects designated as mission critical or whose life cycle costs are greater than $25 million.							

Table 3.1.4 Concept Phase Activities and Documentation Requirements

3.2 Technical Management

Appointed by the CIO, the System Development Manager is responsible for designing, developing, and deploying an AIS. The System Development Manager ensures that the AIS is consistent with the agency's strategic information technology plans and is managed according to sound life cycle management principles and practices. The Project Management Technical Standard and Guideline, IT-212.02-01, describes the responsibilities of the System Development Manager in more detail. In addition, the System Development Manager must:

a. Support the Project Manager,

b. Coordinate with the Office of System Product Assurance to develop a Quality Assurance Plan,

c. Ensure that technical resources are allocated within the constraints of the approved AIS development budget,

d. Develop detailed technical plans and schedules, and

e. Ensure technical performance and adherence to schedule.

Additional information regarding the roles and responsibilities of the System Development Manager is provided in the paragraph 1.9.5 of this Manual and in the Project Management Technical Standard and Guideline, IT-212.2-01.

3.3 System Boundary

The system boundary established the context through which the AIS project addresses the requirements expressed in Business Case or equivalent document. In this sense the development of the system boundary should be considered as a thought process involving several key project management activities and decisions that are usually interdependent and therefore are typically performed concurrently. These activities include:

a. Performing strategic planning,

b. Documenting high level requirements,

c. Determining feasibility,

d. Allocating project resources, establishing a high level project schedule, and

e. Stating assumptions about, and constraints imposed on the project by factors outside the Program Sponsor's or Chief Information Officer's control.

Depending upon project needs and tailoring agreements, system boundary decisions may be recorded in one or several documents. When all of these activities are treated in a single document, that document is referred to as the "System Boundary Agreement." When these topics are treated individually, the system boundary may be expressed in the Project Management Plan, the Requirements Specification, Part 1, and the Concept of Operations document. Regardless of the approach taken, the System Boundary is developed by the Project Manager, with the assistance of the System Development Manager, and is a signed agreement between the Program Sponsor and the CIO affirming a mutual and sufficiently detailed understanding of project requirements, cost, and schedule. Additional instructions for developing a System Boundary Agreement are provided in the System Boundary Technical Standard and Guideline, IT-212.2-10.

3.4 Project Planning

3.4.1 Developing the Project Management Plan

The Project Management Plan serves as a management tool to direct and monitor the progress of system definition, design, development and deployment. The Project Manager, with the assistance of the System Development Manager and the Director, Office of Technical Plans and Policy[5] prepares the Project Management Plan at the beginning of the Concept Phase and revises this plan as necessary, throughout this phase and throughout the life of the project. The Project Management Plan is approved by, and periodically reviewed by both the Program Sponsor and the CIO. The Project Management Plan is also inspected by the Technical Review Board as part of a technical review to ensure that it accurately reflects technical, cost and schedule performance. A sample Project Management Plan is provided in the Project Management Technical Standard and Guideline, IT-212.2-01. Contractors may prepare components of the Project Management Plan, but are prohibited from determining requirements, and from assigning roles, responsibilities, or authority.

[5] The Office of Technical Plans and Policy coordinates project planning, project reviews, and associated program oversight and project monitoring activities; administers baseline project plans; and manages the automated Project Control and Analysis Tool for project tracking; coordinates the development and implementation of agency-wide information technology policy; annual strategic and operational technology plans; and supporting budget submissions.

3.4.2 Developing the Concept of Operations

The Concept of Operations provides organization and business process information. The Concept of Operations provides a high level description of how an organization currently performs its work, how it will perform its work in the future, what people and organizational changes will be required, and what risks are associated with the new or modified AIS. This document also provides a text-based description of business processes within the system boundary and establishes a transition process through which common definitions regarding the current and future business process are documented and managed.

The Project Manager is responsible for developing the Concept of Operations and may be supported by a team of business area experts, as well as experts from other areas such as Human Resources or Facilities. This team defines, develops and documents the current and future business process using textual descriptions, and activity models, process maps, or other tools as appropriate. The Program Sponsor approves the Concept of Operations and ensures that the necessary business policies, procedures, and resources are provided to the process improvement effort in an adequate and timely manner. Refer to the Concept of Operations Technical Standard and Guidelines, IT-212.2-11, for additional details on preparing a concept of operations.

3.4.3 Developing High Level Requirements

High level requirements are contained in the System Boundary Agreement and the Requirements Specification, Part 1. These requirements are based upon opportunities identified in the Business Case or equivalent document and represent a preliminary translation of business requirements into logical data and logical process models. These logical models represent only the essential concepts needed to address a business need and, by intention, do not address technical performance or physical design considerations. The purpose of this translation is to ensure that the project team has a clear understanding of the over-all business requirement that will be implemented before embarking upon detailed analysis and technical design.

High level requirements are expressed as high level entity relationship data models, high level business function decomposition diagrams, high level business process models, business rules and procedures, and other enterprise information. These requirements are deduced from documents such as the System Boundary or the Concept of Operations, and through focus sessions with business area experts.

In many situations it will be advantageous to use automated tools to develop, record, and manage high level requirements. There are a variety of tools available to assist in performing this function, ranging from simple word processors, spreadsheets, and desktop database tools to sophisticated integrated information engineering, and requirements management packages, such as the Requirements Traceability Tool. In selecting the most appropriate tools to perform this task, the System Development Manager should consider the scale, target environment, available resources, available skills, schedule constraints, system integration requirements, AIS implementation tools and consistency with the Technical Reference Model.

The standard OCIO requirements management tool must be used whenever practical. The Office of System Product Assurance will provide technical support to the project in the use of this tool. When it is not practical for the AIS project to use the OCIO standard tool, the Office of System Product Assurance will copy project requirements into the standard requirements management tool.

The following items must be reflected both in the system boundary, the requirements specification, and in the subsequent designs that are derived from these requirements:

a. The purpose of the system including goals, objectives, and critical success factors,

b. Performance measures that are meaningful to the Program Sponsor and end user,

c. Functional needs, as perceived by the user from the business area(s) supported, captured as requirements by business area experts (these requirements are used as the basis for determining feasible alternatives),

d. Assumptions and constraints concerning the business environment within which the system will operate, including legal, security, facility, and labor or work-flow considerations,

e. Assumptions and constraints concerning the technology that may be used, such as conclusions from technology impact analysis, user interfaces, use of the information technology infrastructure, and waivers, and

f. Assumptions and constraints concerning execution of the project, including the budget, schedule, project facilities, acquisition considerations, completion criteria, and the system development process.

High level requirements initially appear in the System Boundary Agreement and are more fully represented in the Requirements Specification, Part 1. Guidance for documenting high level requirements is provided in several Technical Standards and Guidelines including the:

a. System Boundary , IT-212.2-10,

b. Requirements Management, IT-212.3-11, and

c. AIS Life Cycle Process Tailoring, IT-212.2-03.

3.4.4 Developing the Quality Assurance Plan

The purpose of quality assurance planning is to ensure that project activities are visible and appropriately supported, and that project plans and work products, including information engineering models and diagrams, contribute to the delivery of an AIS product that is fit for use and meets customer expectations. The Quality Assurance Plan is initially developed, approved and implemented during the Concept Phase to support this objective. This plan identifies the standards and polices that will apply, identifies the specific work products to be delivered, and establishes the type and schedule of reviews to be conducted in developing or enhancing an AIS.

The Quality Assurance Plan is developed based on the Concept Brief, System Boundary, and the Project Management Plan. These documents determine project size and scope and allocate project resources including support for quality assurance activities. These documents also serve as the basis for tailoring decisions and agreements that are recorded in the Concept Brief and Quality Assurance Plan. These decisions and agreements are intended to establish and document, at an appropriate level of detail, project management, design, development, testing, and support activities. Analysts within the Office of System Product Assurance will assist the System Development Manager by preparing the Quality Assurance Plan. The Project Manager addresses specific quality assurance issues relating to the customer workforce. These issues are outside the scope of the Quality Assurance Plan. The Quality Assurance Plan is prepared by the Office of System Product Assurance, reviewed by the System Development Manager, and is approved by the Technical Review Board as part of the High Level Requirements Review. This plan is updated and reviewed at each phase of the life cycle. Additional guidance on tailoring is provided in the AIS Life Cycle Process Tailoring Technical Standard and Guidelines, IT-212.2-03. Additional guidance on quality assurance planning is provided in the Quality Assurance Technical Standard and Guideline, IT-212.2-04.

3.4.5 Developing Electronic Records Management Requirements

It is appropriate at this stage for the system development manager and appropriate business users to begin assessing high level requirements in 13 electronic records management areas. Not all areas of consideration apply to all AISs. When this is the case, the particular Electronic Records Management (ERM) requirement area should be noted as not applicable to those AISs.

a. *Records Acquisition*, which includes capture of complete electronic records, links to notes and annotations, hyperlinks, and working files, conversion of paper records to electronic form, quality control, quality assurance, and audits of the document capture process.

b. *Record Metadata*, which addresses metadata management and record profile metadata.

c. *File Management*, which covers physical and referential integrity protection.

d. *Preserve Integrity*, which addresses protection against alteration and validating integrity.

e. *Protect Confidentiality*, to ensure that information is not disclosed or revealed to unauthorized persons.

f. *Access Controls and Authentication*, which covers identification and validation of identity.

g. *Search, Retrieval and Reproduction*, which covers such issues as search and retrieval, storing search results, displaying and printing records with indices and annotations, and access privileges.

h. *Audit Trail*, to address use history profiles, their creation and update, and links to other information system tracking or event logging systems.

i. *Vital Records Backup and Recovery*, to cover policies and procedures for disaster recovery.

j. *Records Retention*, which covers retention content, periods, schedules, and disposal procedure.

k. *Migration*, to address the accessibility and transferability of electronic records despite changes in information technology and including copy, reformat, and transfer procedures as well as media management.

l. *Transfer to Permanent Archival Storage*, which describe policy and procedure for long-term retention.

m. *Records Hold*, which covers steps for holding records when litigation, audit or investigation is foreseen.

More detail describing these electronic records management requirement areas can be found in the technical note, "Electronic Records Management: Checklist for Automated Information Systems."

3.5 Defining the High Level Architecture

3.5.1 The System Architect's Role

The Office of System Architecture and Engineering (OSAE) defines and evolves the USPTO-wide information technology infrastructure architecture, ensuring the proper development of that infrastructure while continuing to implement necessary upgrades and integrate applicable new technology. OSAE evaluates and incorporates emerging technologies, standards, and products into the infrastructure Technical Reference Model and develops and/or reviews and approves technical architectural designs for automated information systems. Principal focus areas include controlling the migration to an open systems environment, implementing adequate security measures, upgrading the performance and reliability of infrastructure components, establishing information technology standards, leveraging internet technologies to support USPTO business functions, and establishing remote access capabilities. Additional information regarding the role of the system architect, AIS high level architecture, and detailed design can be found in the High Level Architecture TSG (IT-212.2-12).

3.5.2 Evaluating Commercial Off-the-Shelf Software

"COTS" or "off-the-shelf" software, if used effectively, can significantly reduce AIS delivery time and development costs. System Development Managers should use COTS software whenever feasible. In determining feasibility, AIS managers must make several difficult trade-off decisions in selecting and using a COTS approach. These decisions will have significant, long-term impact on the cost for developing and operating the AIS. The Project Manager, the System Development Manager, and the Systems Architect must carefully consider the benefits and disadvantages of using COTS software products when preparing an economic analysis or designing a high level architecture.

The benefits and costs associated with using COTS software must be identified in terms of several key characteristics including uses, packaging, and acquisition agreements. This will allow managers to better understand the costs associated with acquiring a COTS solution, and will also assist in determining the costs of activities associated with the integration, maintenance, and operational support of COTS products.

There are at least five major ways COTS can be characterized according to use:

a. Office automation systems (e.g., word processing, spread sheets, presentation tools, electronic mail).

b. Application systems (e.g., human resources, financial management, payroll, project management).

c. AIS production support packages (e.g., data base management systems, document management systems, report generators, search tools, work flow).

d. System and network management (e.g., operating systems, help desk tools, software distribution tools, system performance monitors, security tools, network monitors).

e. System analysis, design, and development and maintenance tools (e.g., I-CASE tools, compilers, test tools, configuration management, requirements management, and data modeling).

There are at least three ways COTS can be classified in terms of packaging:

a. Highly specialized software modules (e.g., image viewers, bar code printing drivers),

b. Groups of interrelated software functions that the manufacturer integrates into software environments (e.g., windows, desk-tops), and

c. Turnkey products (e.g., high speed image capture scanners and software, point of sales registers and software).

It is also important to consider the terms and costs for COTS acquisition such as:

a. Types of support service vendor provides (e.g., training, special modifications, consulting, remote diagnostics),

b. Pricing structure (e.g., site licensing, upgrade pricing, support costs, volume discounts),

c. Composition (e.g., incremental acquisition of functional components, bundling/unbundling of options), and

d. Product format (e.g., source code, executable code, or network service provider).

3.5.3 Benefits of Using COTS Software

A major advantage of COTS software products is that these products come already developed and tested. Frequently, a large number of commercial customers are able to use and evaluate specific COTS products in an operational environment, and based upon their experiences, provide constructive comments to the manufacturer. As a result, COTS products come with many practical, user-driven, enhancements included. This translates into an immediate gain in functionality, usability, and reliability. Also, because a large number of commercial users share in the total costs to develop, market, distribute, and support COTS products, vendors are able to keep unit costs to a level that is affordable to the individual customer.

3.5.4 Disadvantages of Using COTS Software

No COTS solution provides all, or the exact business functionality that the user needs. A comprehensive solution to a business area requirement may require that integrated COTS approaches be supplemented with in-house software. Generally, COTS products are difficult to modify internally. When the only alternative is to modify a COTS product, it is usually at significant risk to the vendor and, as a result, great cost to the customer. The System Development Manager must be aware of the costs, time, and level of effort necessary to select and integrate COTS software into the overall AIS. Due to issues relating to the cost of flexibility, compatibility, functionality, or control over source code, the System Development Manager may determine that the most economically feasible way to address a requirement is through in-house development.

3.5.5 Selecting an Approach

The System Development Manager must be aware of several key factors when deciding whether to develop software in-house or whether to purchase and integrate a COTS product.

a. Business Focus and Potential for Reuse -- if there is a reasonable chance that the needed AIS functionality is reusable on several other applications then it may become very practical to develop this functionality in-house. Reuse provides almost all the benefits expected of COTS products such as labor and development cost savings, and rapid implementation, plus many of the benefits expected from software developed in-house including flexibility and controllability. The System Development Manager must ensure that all reusable components, including requirements, specifications, and designs are placed in a CM repository for reuse.

b. Compatibility with the Technical Reference Model -- if the only COTS products needed and currently available are incompatible with the Technical Reference Model, then the System Development Manager should consider developing an in-house approach that is compatible with the Technical Reference Model.

c. Cost of Integration and Maintenance -- Integration costs may be higher for COTS products, while maintenance cost will be higher for in-house development. However, both in-house developed functionality and COTS provided functionality will have full life cycle costs. Poor performance by the manufacturer in designing, developing, testing, and supporting COTS products will result in higher costs to the AIS development organization.

d. Reputation, Market Share, and Quality of Manufacturer Services -- System Development Managers must consider the long term viability of COTS software. Software firms that stand behind their products, look to establishing a long term presence in their markets, and look to increasing market share will provide COTS products to their customers that are less costly to operate, enhance, and maintain. This does not mean that there will not be problems from time to time. It just means that software firms that do not live up to customer expectations will eventually suffer loss of credibility in the market. This in turn provides some indication of the long-term costs the AIS project will incur for COTS maintenance, enhancement, integration, and support.

3.6 Assessing the Information Technology Investment

When the USPTO spends money on information technology, it is an investment in improving the quality and value of the agency's business performance. Senior management must assess the business worth of an AIS project in terms of the changing needs of the business, and in terms of advances or changes in technology or services. Moreover, each AIS project must be evaluated in the context of the portfolio of all AIS projects during the strategic information technology planning process to ensure that there is a strong business case for developing and deploying the new capability.

> *Each AIS project must be evaluated in the context of the portfolio of all AIS projects to ensure that there is a strong business case for developing and deploying the new capability.*

When making an information technology investment, the Program Sponsor and CIO must be in agreement that project expectations are realistic and achievable. This agreement, documented as part of the system boundary, must be revisited and reaffirmed several times throughout the life of an AIS project. If there are any significant changes in business requirements, project resources, or project schedule, the system boundary and supporting economic analysis must be revised.

To help determine whether the AIS project is a worthy investment and to identify the preferred approach, the Project Manager, with the assistance of the System Development Manager, identifies and evaluates various alternative approaches. This systematic process, called an economic analysis, compares the costs and benefits of alternatives that are potentially feasible. An economic analysis must be prepared for each AIS project designated as mission critical. There must be at least two feasible alternatives considered in the economic analysis - the current system and the proposed system(s). The Economic Analysis Technical Standard and Guideline, IT-212.2-13, provides guidance for preparing an economic analysis.

3.7 Project Risk Management

The Project Manager must continually identify AIS project risks and identify ways to reduce these risks to acceptable levels. During the Concept Phase these risks are primarily concerned with establishing a realistic commitment to addressing AIS project requirements and obtaining the resources necessary to achieve project goals. The Project Manager will advise the Program Sponsor, the CIO, and the Systems Development

Manager on matters of significant risk and will coordinate risk management activities with key managers and analysts based upon their ability to control risk.

3.7.1 Project Risk Assessment

The intent of this guideline is to establish a level of project risk assessment, planning, and management that is appropriate to the nature of the work that is expected to be performed using the AIS.

Continual analysis[6] of the existing project situation will be conducted to identify significant AIS project risks. Primary consideration will be given to identifying business and project risks, including major uncertainties in specifying or satisfying system boundaries (i.e., requirements, costs, and schedule). Some of the most common business and project risks encountered in the Concept Phase are associated with:

a. Replacement of key managers or loss of sponsorship,

b. Loss of funding,

c. Change in mission,

d. Reorganization, and

e. Unclear leadership structure and back-up process for key personnel.

The Project Manager and the System Development Manager will identify all significant business and project risks to the best of their ability. These managers will estimate and evaluate significant business and project risks, and will provide some brief discussion of pragmatic approaches they might take should any of these risks materialize into a situation that could adversely impact the project. There are three major sources of project risk that the Project Manager must consider:

a. Availability of detailed and complete project information,

b. Sufficient project time and project resources, and

c. Sufficient project control.

[6] The Project Manager should exercise care to differentiate between *project risk analysis* and *security risk assessment*. Many AIS projects analyze the risk of failing to successfully complete the project -- a different activity from security risk assessment. Though both activities share many common traits and underlying principles, *security risk assessment* focuses more upon ensuring the integrity, availability and confidentiality AIS components including business information and business processes.

The intent of this guideline is to establish a level of project risk assessment, planning, and management that is appropriate to the nature of the work that is expected to be performed using the AIS. Excessive, duplicative, or unnecessary risk management should be avoided. Project Managers and System Development Managers are encouraged to reuse or adopt already existing risk management practices, policies, procedures, and mechanisms whenever practical. It is vitally important that the Project Manager is fully aware of business and project risks in terms of actual damage, cost of prevention, and cost of corrective measures. Information used to identify, estimate, and evaluate significant risks will be documented.

3.7.2 Project Risk Review and Mitigation

The Project Manager presents project risk assessment findings to the Program Sponsor, Technical Review Board, or the CIO, as needed during the course of the AIS project.

Risk considerations will be part of normal business and will reaffirm the significance of risks. To illustrate, risks associated with the High Level Architecture should be identified and presented during the High Level Requirements Review. The Project Manager should solicit management support for addressing significant risks. Based upon the recommendations of the Project Manager, the Program Sponsor or the CIO may assign additional staff or allocate additional resources to reduce or avoid significant risks. Additional guidance for managing project risk can be found in the risk management section within the Project Management TSG (IT-212.2-01).

3.8 AIS Security

While USPTO, OCIO, and issue-specific security policies address security from a broad perspective, the formulation and full implementation of these policies is independent of the life cycle and generally beyond the control of any individual project manager. As a rule, these organizational security policies do establish general security goals and objectives, but they do not provide sufficient information or direction necessary to implement specific AIS security measures. For this reason, the Project Manager must consider project level security planning for each AIS project and/or PTOnet infrastructure project. The Project Manager must work closely with the security analysts in the Office of Information Systems Security (OISS) to accomplish project level security planning.

The processes of security planning and risk management share many common activities and purposes. For example, a collateral benefit derived from analyzing and managing risks, is that project managers are aware of AIS assets (e.g., data, hardware, software, facilities, etc.) and are able to anticipate specific events that could compromise the integrity of those assets, render those assets unavailable to the end-user, or render those assets unfit for service. Risk assessment and management also provides project managers with an understanding of functional and technical management's willingness to accept a broad range of risks, including security risk. Based upon this knowledge, project managers are able to develop cost-effective project-level security plans, policies, and procedures that meet business needs.

Some of the most commonly thought-of AIS security issues include:

a. AIS back-up, contingency, and disaster recovery,

b. Data center security planning,

c. Security test and evaluation, and

d. Security certification and accreditation or interim authority to operate[7].

3.8.1 Concept Phase Security Activities

Like most other aspects of AIS life cycle management, security is most effective and efficient if planned and managed throughout the AIS life cycle. During the Concept Phase, the System Development Manager develops early conceptual designs of anticipated AIS security features. Typically, due to the fact that the AIS is early in its life cycle, these designs are not supported by detailed requirements but are based upon a common sense understanding or "sensitivity assessment" of the business and the underlying security needs[8].

3.8.2 Sensitivity Assessment

A sensitivity[9] assessment looks at the value of AIS data/information and the AIS itself to USPTO. This assessment should consider financial impact, legal implications, USPTO

[7] Based upon the recommendation of the Project Manager and the System Development Manager, the CIO may grant a security certification and accreditation or an interim authority to operate at the end of the Development Phase.

[8] These early conceptual designs are informal and are simply used to facilitate the development process in much the same manner that prototypes are used. These designs will be further modified, refined, and formalized as firm requirements are identified and developed.

[9] The definition of *sensitive* is often misconstrued. *Sensitive* is synonymous with *important* or *valuable*. Some information is sensitive because it must be kept confidential. Much more information, however, is sensitive because its integrity or availability must be assured. The Computer Security Act and OMB Circular A-130 state that information is sensitive if its unauthorized disclosure, modification (i.e., loss of

policy (including federal and Department of Commerce policy), and the functional needs of the business. Sensitivity is normally expressed in terms of integrity, availability, and confidentiality. Project management must consider such factors as the importance of the AIS to USPTO's mission and the consequences of unauthorized modification, unauthorized disclosure, or unavailability of AIS information when assessing sensitivity. To address these types of issues, it is essential that those USPTO business partners who will use the AIS participate in this assessment.

In performing a sensitivity assessment, project management must address the following questions:

a. What information is handled by the system?

b. What kind of potential damage could occur through error, unauthorized disclosure or modification, or unavailability of information or use of the AIS?

c. What laws or regulation affect security (e.g., The Privacy Act or the Fair Trade Practices Act)?

d. To what threats is the AIS or AIS information particularly vulnerable?

e. Are there significant environment considerations (e.g., hazards associated with AIS location - for example, next to an airport or railroad office)?

f. What are the security-relevant characteristics of the AIS end-user community (e.g., level of computer or AIS sophistication and training, security clearances, etc.)?

g. What internal security standards, regulations, or guidelines apply to this AIS?

The sensitivity assessment starts an analysis of security that continues throughout the life cycle. The assessment helps determine if the AIS project needs special security considerations, if further analysis is needed before committing to begin the next phase of the LCM (to ensure feasibility and reasonable cost), or in rare instances, whether the security requirements are so strenuous and costly that system development or acquisition will not be pursued. The sensitivity assessment can be another planning document or may be combined with the System Boundary Agreement, Requirements Specification, or Project Management Plan according to tailoring agreements reached between AIS project management and the Office of System Product Assurance.

integrity), or unavailability would harm the agency. In general, the more important a system is to the mission of the agency, the more sensitive it is.

3.9 Acquisition of Information Technology Resources

Acquiring information technology resources is often a difficult task that requires knowledge, experience, the ability to work effectively with people, good judgment, and common sense. The process is mandated by regulations designed to ensure that USPTO acquires only what is needed, and that USPTO considers and makes use of existing resources, including Department of Commerce and other agency programs and contracts. When a procurement action is determined to be appropriate, the acquisition process attempts to ensure full competition among vendors and to prevent abuses. USPTO strategies for acquiring information technology products and services are contained in the most recent version of the Strategic Information Technology Plan. All AIS managers should have a fundamental grasp of federal, departmental, and USPTO Information Resource policies and procedures.

AIS project managers must coordinate with the Office of Acquisition Management throughout the AIS life cycle to acquire information technology products and services. The goals of acquisition management are to ensure that:

a. The information technology is appropriate to the needs of the organization,

b. Procurements are consistent with the Technical Reference Model and the overall architectural concept,

c. Information technology components are interchangeable and interoperable,

d. Information technology procurements are performed according to Federal acquisition laws and regulations,

e. Information technology procurement plans are well documented,

f. Information technology procurement plans encourage small business participation,

g. Procurements rely on GSA schedules and government-wide contracts, and

h. Procurements enable contractor end-to-end responsibility.

The Office of Acquisition Management directs the acquisition of information technology hardware, software, and support services. This office ensures that information technology acquisitions are conducted in a manner that is consistent with USPTO's strategic information technology plans. The Office of Acquisition Management provides acquisition management support services, including Contracting Officers' Technical Representatives functions for USPTO-wide information technology support service contracts. The Office of Acquisition Management also advises and assists in the administration of other information technology contracts.

3.10 Project Management Plan Update

The Project Manager must update the Project Management Plan in preparation for the High Level Requirements Review. This update will include a refinement of the project schedule with special emphasis on the Detailed Analysis and Design Phase. This update must also include completion of initial plans for AIS development, configuration management, quality assurance, security, risk management, and data management prepared in accordance with the applicable Technical Standards and Guidelines. The Technical Review Board must review and approve the updated Project Management Plan before the System Development Manager can officially begin the Detailed Analysis and Design Phase.

3.11 Concept Approval

3.11.1 Project Manager and System Development Manager Evaluate Documentation

The Project Manager and the System Development Manager evaluate the System Boundary Agreement, Project Management Plan, Quality Assurance Plan, Concept of Operations, Security Plan, Data Management Plan, Configuration Management Plan, Requirements Specification, Part 1, High Level Architecture, and all supporting initiatives and plans and assess the following:

a. Conformance to requirements and business needs,

b. Conformance to standards and guidelines, and

c. Technical and economic feasibility.

Based upon the findings of this evaluation, the Project Manager and the System Development Manager will submit these plans to the Technical Review Board for approval at the High Level Requirements Review.

3.11.2 High Level Requirements Review

Before beginning analysis to elaborate detailed requirements, the Project Manager will ensure that the project team and the users who generated those requirements reach consensus on their interpretation. A technical review will be conducted in accordance with procedures in IT-212.2-04, Quality Assurance, to provide a basis for support planning in the Detailed Analysis and Design Phase and to establish the foundation for technical reviews throughout the remainder of the AIS life cycle. The Concept Phase is completed upon approval by the Technical Review Board at the High Level Requirements Review and the Program Sponsor and CIO agree to the system boundary.

Before beginning analysis to elaborate detailed requirements, the Project Manager will ensure that the project team and the users who generated those requirements reach consensus on their interpretation.

INITIATION PHASE

2.1 Introduction

2.1.1 Purpose

The Initiation Phase begins when management determines that it is necessary to enhance a business process through the application of information technology. The purposes of the Initiation Phase are to:

a. Identify and validate an opportunity to improve business accomplishments of the organization or a deficiency related to a business need,

b. Identify significant assumptions and constraints on solutions to that need, and

c. Recommend the exploration of alternative concepts and methods to satisfy the need.

2.1.2 Overview

During the Initiation Phase the Program Sponsor designates a Project Manager, and obtains project funding and resources. The Project Manager, in coordination with the business area, must concentrate on identifying opportunities to improve business operations and must assist the Program Sponsor in documenting these opportunities in the Business Case. AIS projects may be initiated as a result of business process improvement activities, changes in business functions, or advances in information technology. The Initiation Phase is completed and the AIS project is begun upon the agreement of the Program Sponsor and CIO.

The Project Manager must concentrate on identifying opportunities to improve business operations.

2.1.3 Tasks

The tasks to be completed during this phase are:

a. Establish project sponsorship,

b. Establish project management,

c. Identify expected range of costs and benefits,

d. Identify opportunities to improve business functions,

e. Identify alternatives that may address the need,

f. Identify programmatic and technical risks,

g. Commit project funding, staff and resources, and

h. Prepare a Business Case.

2.1.4 Activities and Documentation

Initiation Phase activities and documentation requirements as summarized in the following table must conform to the indicated Technical Standard and Guidelines or other standards as noted. Published standards and guidelines may be augmented with Tailoring Agreements.

Work Product	TSG / Standard	Who's Responsible	Must Create	Should Update	Must Update	Base-line	Must Complete
Business Case	IT-212-.2-13	Program Sponsor, Project Manager	X				

Table 2.1.4 Initiation Phase Activities and Documentation Requirements

2.2 Project Management

2.2.1 Establishing Program Sponsorship

The Program Sponsor is the principle authority on matters regarding the expression of business needs, the interpretation of functional requirements language, and the mediation of issues regarding the priority, scope and domain of business requirements. The Program Sponsor is the senior spokesperson for the project, and is responsible for ensuring that the needs and accomplishments within the business area are widely known and understood. The Program Sponsor is also responsible for ensuring that adequate resources to address their business area needs are made available in a timely manner. A strong Program Sponsor is critical to the success of an AIS project. Additional information regarding the roles and

A strong Program Sponsor is critical to the success of an AIS project.

responsibilities of the Program Sponsor is provided in Chapter 1 of this Manual and in the Project Management Technical Standard and Guideline, IT-212.02-01.

2.2.2 Appointing the Project Manager

The Program Sponsor appoints the Project Manager. The Project Manager is responsible for:

a. Supporting the Program Sponsor,

b. Ensuring that all business aspects of the AIS project, including business area transition planning and appropriate training, are supported in the Project Management Plan,

c. Establishing detailed project plans and schedules,

d. Working with the CIO and the CFO to ensure that project funding and resources are made available, and

e. Ensuring that project funding and resources are allocated within the constraints of the approved project budget.

The Program Sponsor should plan for the Project Manager to be assigned until the project is completed. This provision is intended to promote continuity, responsibility, and accountability. Additional information regarding the roles and responsibilities of the Project Manager is provided in Chapter 1 of this Manual and in the Project Management Technical Standard and Guideline, IT-212.02-01.

2.3 Preparing the Business Case

The Business Case describes a desired improvement to a business process in purely business terms. This document provides background information that describes why a business process improvement is necessary and what business benefits can be expected by implementing this improvement. The Project Manager will assist the Program Sponsor in preparing the Business Case and identifying detailed opportunities for business process improvements. The CIO will assist the Program Sponsor in developing the Business Case by providing a preliminary range of cost and schedule estimates for information technology development and support

> *The Business Case describes a desired improvement to a business process in business terms.*

activities. Other PTO decision memoranda such as Executive Committee Decisions can also be used to initiate a project.

2.3.1 Providing Background Information

The Business Case must provide background information at a level of detail sufficient to familiarize senior managers with the business opportunities that can be realized through leveraging information technology. A business scenario and context must be established in which a business problem is clearly expressed in business terms. Care must be exercised, however, not to provide too much detail at the expense of clearly and concisely stating the business need.

2.3.2 Organizing the Business Case

The Business Case identifies items as listed below. Detailed information regarding development of the Business Case can be found in the Economic Analysis TSG, IT-212.3-13, Appendix B.

a. Provide the title of the project

b. Provide a high level description of what business function is being performed, why this information technology project is being undertaken and its strategic direction, what is to be done, and identify efforts to re-use what has already been done by other projects,

c. Commitments, benefits, and performance measures,

d. Project schedule and cost

e. Other issues or considerations impacting the decision.

The CIO will ensure that the Strategic Information Technology Plan is revised to incorporate the AIS project.

OPERATIONS PHASE

7.1 Introduction

7.1.1 Purpose

The purposes of the Operations Phase are to:

a. Operate, maintain, and enhance the AIS,

b. As required, certify that the AIS or infrastructure system can process sensitive information in accordance with appropriate regulations,

c. Conduct periodic AIS or infrastructure system assessments to ensure the functional requirements are being satisfied, performance measures identified in the system boundary are achieved, and

d. Determine when the AIS or infrastructure system should be modernized, replaced, or retired.

Production Managers are encouraged to work closely with end users and System Maintenance Managers and continually investigate ways to improve AIS or infrastructure system functionality, and ensure that the system continues to address current business needs.

Production Managers are encouraged to work closely with end users, System Maintenance Managers, and AIS and infrastructure support groups to continually investigate ways to improve AIS functionality, and ensure that the AIS continues to address current business needs.

7.1.2 Overview

The AIS or infrastructure system is operated, maintained, and enhanced as appropriate to support the intended business function.

7.1.3 Tasks

The tasks to be performed during this phase are:

a. Operate the AIS or infrastructure system.

b. Conduct a Post Installation Review when requested.

c. Control all changes and maintain the AIS or infrastructure system, as required, during its remaining life.

d. Ensure the availability of resources in the budget for AIS or infrastructure system operation, maintenance, and modernization.

e. Ensure continued enforcement of installed system security safeguards.

f. Review and revalidate the functional utility of the AIS or infrastructure system and the adequacy of the technical design.

g. Collect reports of problems and ensure appropriate corrective action is taken.

h. Collect and respond to requests for new or changed AIS or infrastructure system functionality.

i. Coordinate AIS or infrastructure system modifications with changes to business processes.

j. Evaluate whether new information technology can be cost-effectively applied to improve AIS or infrastructure system performance and capacity.

k. Periodically test the effectiveness of disaster recovery procedures and test to ensure the recoverability of the AIS or infrastructure system within service commitments.

l. Measure and monitor the system's effectiveness in achieving performance objectives identified in the Service Level Agreement.

m. Maintain each reusable component stored in the USPTO Enterprise Repository.

n. Perform data quality monitoring to ensure data integrity.

This phase is complete when the system is retired or replaced.

7.1.4 Activities and Documentation

Operation Phase activities and documentation requirements as summarized in the following table must conform to the indicated Technical Standard and Guidelines or other standards as noted. Published standards and guidelines may be augmented with Tailoring Agreements.

Work Product	TSG / Standard	Who's Responsible	Must Create	Should Update	Must Update	Base-line	Must Complete
Update earlier documents. Documents developed during the project life cycle may need revision due to requirements changes, new technology, or other reasons. Because each phase of the life cycle builds upon the earlier phases, updates to earlier approved document may be required to support the process.				X			
Update Operational Support Plan	IT-212.5-01	System Development Manager			X		

Table 7.1.4 Operation Phase Activities and Documentation Requirements

Any plan or work product could be impacted as a result of an AIS or infrastructure system modification. Even though these modifications may occur in the Operation Phase, it is critically important from maintenance, operation, and support perspectives that the AIS or infrastructure system structure, procedures, configuration information, and training documentation be kept current and complete. The Technical Standards and Guidelines governing the content and form of plans and work products during the Initiation, Concept, Detailed Analysis and Design, or Development Phases will continue to apply throughout the Operations Phase.

7.2 Post Installation Review

A Post Installation Review (PIR) should be conducted when there are remaining discrepancy reports, deferred requirements for future maintenance release, or any issues related to the system operation. The TRB or Project Manager may request that a PIR be conducted. An independent Operational Assessment, coordinated by the Office of System Product Assurance, may also be conducted in the Operations Phase. Independent testing, performed as part of the Post Installation Review or Operational Assessment, will be conducted independently o the development organization. Defects uncovered by this testing may lead to change in the work products created in then previous phases. The technical standard and guidelines for those phases apply, as needed, during the Operations Phase.

The Production Manager will select the Post Installation Review Team from within the end user community. The Production Manager will also set the schedule for the Post

Installation Review and will determine the scope and duration of this review. The Post Installation Review Team may conduct testing of the AIS or infrastructure system. The Post Installation Review Team is strongly encouraged to examine user training courses and materials, user manuals and guides, as well as error messages, help message and prompts from the perspective of usability, completeness, accuracy, and ease of comprehension.

7.3 AIS or Infrastructure System Operational Support

7.3.1 Operational Services

Critical information contained in the OSP must be described, such as the hours of availability, performance objectives, system backup, disaster recovery, security auditing, and preventive maintenance services as outlined in the Service Category Forms provided in the Operational Support TSG.

7.3.2 Problem Reporting and the Help Desk

Users experiencing difficulties with the AIS or infrastructure system should phone the Help Desk (703-305-9000). The user reporting a problem should describe the nature, urgency, and severity of the problem. To facilitate future handling of the problem report, the user reporting a problem is strongly encouraged to record the problem number provided by the Help Desk. The Help Desk will first attempt to verify that the AIS or infrastructure system is actually not functioning as intended. Problem resolution responsibilities are defined in the Operational Support Plans of each system. Additional guidance on problem reporting and Help Desk support can be found in the *Help Desk Services Guide*.

7.4 Meetings to Obtain User Feedback

User Feedback Meetings will be conducted by the Production Manager and supported by the Office of the Chief Information Officer as needed. The first User Feedback Meeting should be held no later than six months after the AIS or infrastructure system (or a major subsystem of the AIS) has been deployed. The User Feedback Meeting should:

The User Feedback Meeting should determine the effectiveness of training, operations, maintenance, facilities, continuity of operations, and supporting documentation.

a. Identify AIS or infrastructure system modifications needed to support the current business process.

b. Determine the effectiveness of the AIS or infrastructure system in meeting customer expectations.

c. Confirm that the AIS or infrastructure system meets the performance measures stated in the system boundary or Requirements Specification.

d. Verify that AIS or infrastructure system capacity and performance, including hardware, software, and telecommunication, are adequate to support the current business process and anticipated growth.

e. Evaluate the opportunity to apply new information technology to meet the business need or to improve system performance.

f. Verify that operational support of the AIS or infrastructure system is acceptable.

g. Determine the effectiveness of training, operations, maintenance, facilities, continuity of operations, and supporting documentation.

h. Evaluate the effectiveness of the life cycle management processes and gather information that can be used to improve those processes.

The results of the User Feedback Meeting must be documented in memorandum form and submitted to the Program Sponsor and the CIO for review.

7.5 Maintenance and Modification

7.5.1 Determination of Requirements

Modification actions can result from a problem report, a request for new or changed functionality, an Operational Assessment, and new release of a COTS product, or a User Feedback Meeting. The Production Manager and System Maintenance Manager examine change requests and problem reports to identify new AIS or infrastructure system requirements, determine approaches to provide corrections to existing functionality, and establish priority for AIS or infrastructure system modifications.

It is very important that changes be restricted in scope and level of effort. This will significantly reduce the risk that implementing the change will result in disruption in services or business operations.

It is very important that changes be restricted in scope and level of effort. This will significantly reduce the risk that implementing the AIS or infrastructure system change will result in disruption in services or business operations. If the requested change appears to involve significant changes to the existing System Boundary, Requirements Specification, or High Level Architecture, then the Program Sponsor should establish a new AIS project to manage the change.

Because there is no easy way to distinguish between system performance issues, modifications, and enhancements, management always determines the classification of a change. For this reason users and operators should work with their respective Production and System Maintenance Managers to determine an approach for implementing changes to software.

7.5.2 Change Requests

Information regarding change requests can be found in the *EAMS User's Guide*. Change requests will contain the following information:

a. A description of the modification.

b. The reason the modification is required and the impact on the user community if the modification is not performed.

c. The input and data that will be affected by the proposed modification.

d. The output (reports) that will be affected by the proposed modification.

e. Priority of the modification.

f. Proposed date and time of modification implementation.

g. Back out procedures.

h. Testing procedures and results.

i. Customer notification plans.

j. Description as to how the modification will impact the users, both during implementation and after implementation.

7.5.3 AIS or Infrastructure System Modification Releases

Because modifications often have an impact on more than one portion of a system, the System Maintenance Manager must implement release procedures for managing AIS or infrastructure system modifications. A release is a well-defined, carefully selected grouping of modifications and non-emergency problem fixes that are evaluated, developed, tested, and implemented at the same time. The Production Manager and the System Maintenance Manager specify the procedures for managing releases in the project's Configuration Management Plan (see Configuration Management TSG, IT-212.2-06).

Releases will be implemented as specified in the project's Configuration Management Plan.

7.5.4 Processing Change Requests

The System Maintenance Manager serves as the focal point for processing change requests and may either initiate changes, or receives, review, and forward requests for change from the Production Manager.

a. The System Maintenance Manager will review the change requests, analyze the resource requirements, and provide an impact statement in accordance with paragraph 7.5.5.

b. The Production Manager and the System Maintenance Manager jointly define the content of releases.

c. The System Maintenance Manager performs the Detailed Analysis and Development activities necessary to modify the AIS or infrastructure system as requested. Documentation needed to perform, support, and use the modification will be updated in accordance with configuration management policies and procedures.

d. Modifications will be thoroughly tested as specified in the Testing Technical Standard and Guideline, IT-212.3-01, before being placed in production. The Production Manager will ensure that users are aware of AIS or infrastructure system modifications and understand how they are used. The System Maintenance Manager will ensure that all requirements, analysis, design, development, and testing documents have been revised according to the applicable Technical Standards and Guidelines, and that help desk and operations personnel have been trained on the changes.

e. All modifications will be placed into production in accordance with configuration management procedures after successful testing and acceptance. The Production Manager and the System Maintenance Manager establish the delivery schedule and priority of release components. Documentation revisions will be included with the release. Emergencies will be handled according to section 7.5.6 of this document.

7.5.5 Estimating Change Resources and Impact

For maintenance of existing AIS's or infrastructure systems, once the Production Manager and the System Maintenance Manager determine change requirements, the System Maintenance Manager:

a. Maintains accurate and complete records of the AIS or infrastructure system change activity, and ensure that these records are traceable to the initial change request or problem report(s).

b. Meets with system analysts and programmers to analyze the needed change or problem, and develop an approach.

c. Estimates the skills, staff, and time needed to make the change and deploy the modification.

d. Analyzes the modification to determine technical requirements and available computing resources such as:

- Processing load the AIS modification is expected to have on existing hardware, system software, and telecommunications.
- Available processing capacity of existing hardware, system software, and telecommunications.
- Needed changes to data structures or data definitions.

- Technical mechanisms needed to ensure protection of sensitive or classified information.
- Needed changes to ensure that the modified AIS Security is certified and AIS security documentation is current.

7.5.6 Prioritizing Change Requests

The Production Manager, System Maintenance Manager, AIS or infrastructure system maintenance organization, and the test team must work closely together in determining the priority and delivery schedule for change requests. The Program Sponsor must determine the priority of the modification requested. The System Maintenance Manager and test team will make exceptions to this rule if there is an emergency.

The Production Manager, System Maintenance Manager, AIS maintenance organization, and the test team must work closely together in determining the priority and delivery schedule for change requests.

7.5.7 Change Request Procedures

In response to a request to modify or repair an AIS or infrastructure system, the Office of System and Network Management, the Office of Data Management, the System Maintenance Manager, and the test team will:

a. Perform the change activities necessary to repair or modify the AIS or infrastructure system to a fully operational status based on the agreed priority.

b. Test changes to the AIS or infrastructure system based on the severity of the problem or the extent of changes required according to the respective Test Plan (see Testing TSG, IT-212.3-01).

c. Provide updated AIS or infrastructure system modification or problem resolution status to the Production Manager according to the Operation Support Plan (see the Operational Support TSG, IT-212.5-01).

d. Develop, test, and deploy changes to the AIS or infrastructure system as specified in the respective Configuration Management Plan (see the Configuration Management TSG, IT-212.2-06).

The problem solving approach applied in implementing AIS or infrastructure system change is essentially the same as that taken for the development of a new AIS or infrastructure system. The primary difference is that the level of effort and risk associated with a modification or maintenance task is generally much smaller than that for developing a complete AIS or infrastructure system. As a result AIS or infrastructure system modifications and maintenance activities require much less review and approval. However, it is still important to ensure that all support groups, analysts, and future maintenance programmers are aware of their responsibilities. It is also extremely important to keep all requirements, design, and development documentation current and complete. This will help ensure that analysts and developers can continue to maintain and modify the AIS or infrastructure system as required.

The System Maintenance Manager will notify the System Development Manager regarding known defects in a deployed subsystem of an AIS or infrastructure system that is under development. The System Development Manager will ensure that the development team corrects these defects in the development environment. This will prevent these defects from reoccurring in a future release of the subsystem.

7.5.8 AIS Change Documentation

Documents needed to specify, design, develop, implement, or test an AIS or infrastructure system modification will be updated. Each documentation change should be identified and referenced to the change request under which the modification is being performed. Specifically, it may be necessary to the revise existing documentation as a result of implementing a modification to an AIS or infrastructure system.

7.6 AIS or Infrastructure System Security

Many security activities take place during the Operations Phase. In general, these activities fall into three areas: security operations and administration, operational assurance, and periodic re-analysis of AIS or infrastructure system security. The Automated Information System Security Controls Manual, IT-212.2-15 provides additional information on managing AIS security during the Operations Phase.

The Information Technology Security Officer will work closely with the Production Manager, the System Maintenance Manager, and the CIO to update security documentation, certification, and accreditation as required. The Test Team is responsible for reviewing test specifications and procedures, and for performing Acceptance Testing.

7.6.1 Security Operations and Administration

Security operations and administration must be performed continually during AIS or infrastructure system operation. Examples of security operation and administration activities include performing AIS or infrastructure system information and system backup, holding security awareness training classes, managing passwords and cryptographic keys, maintaining user access privileges and access rights, and updating security software controls. Security operations and administration touches on virtually every aspect of the LCM and requires support from numerous OCIO organizations. The System Maintenance Manager must ensure that the AIS or infrastructure system documentation remains current and reflects appropriate levels of security operations and administration.

7.6.2 Operational Assurance

Operational assurance is the process of reviewing an operational AIS or infrastructure system to ensure that security controls, both automated and manual, are functioning correctly and effectively over time. To maintain operational assurance, security analysts can perform security audits and security monitoring as a way to ensure that security controls continue to be effective[1].

7.6.3 Periodic Re-Analysis of AIS or Infrastructure System Security

Periodically, it is useful to formally re-examine AIS or infrastructure system security from a broad perspective. This analysis may lead to a re-accreditation should help ensure that AIS or infrâstructure system security is still sufficient, and should help identify the need for major security changes or enhancement (either automated or manual).

This analysis should address both the high level security and management concerns of senior management as well as the implementation of security controls. It is not always necessary to perform a security risk assessment or certification in conjunction with this activity, but these activities do share many common characteristics and it is frequently cost effective to perform both concurrently. Naturally, if there have been significant and extensive changes to the AIS or infrastructure system since the last security analysis, additional effort should be expended to fully evaluate the operational effectiveness of related security controls. System security testing must be performed on any AIS or infrastructure system changes that are implemented in software as a result of a periodic security analysis. As in a security accreditation, the CIO and the Program Sponsor should issue a memorandum accrediting security and explicitly accepting risk, or reissue a interim authority to operate. Section 6.3 of this Manual provides additional guidance on the accreditation process.

[1] A *security audit* is generally a one-time or periodic event to evaluate security, whereas *security monitoring* is an on-going activity that examines either the AIS, or business and operational practices.

7.7 AIS or Infrastructure System Retirement

An AIS or infrastructure system that no longer serves a valid business need, has been included or incorporated into another AIS or infrastructure system, or has been replaced by a more effective or efficient solution (either technical or procedural) should be removed from the workplace and from the operational environment. Even though there may no longer be a business need for an AIS or infrastructure system, there may continue to be a significant need to protect sensitive information previously managed by that AIS or infrastructure system. The Information Technology Security Officer will provide consultation and support to the Production Manager and the System Maintenance Manager to prevent the unauthorized destruction, disclosure, or modification of this data. On retirement, documentation will be updated accordingly.

Either the Program Sponsor or the Senior Executive within the business area supported by the obsolete AIS or infrastructure system may officially retire that AIS or infrastructure system with a brief memorandum to the CIO.