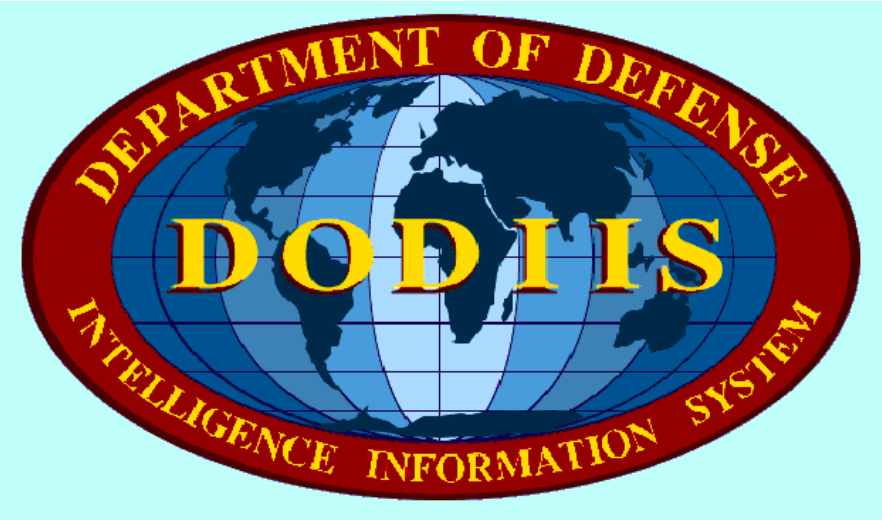

Test and Evaluation Policy

for

Department of Defense Intelligence Information System (DoDIIS) Intelligence Mission Applications (IMA)

April 1999

Prepared by: DExA for Test & Evaluation (T&E)
497th Intelligence Group /INDS
240 Luke Ave, Bldg. 1304
Bolling AFB, DC 20332-7030
(202) 404 - 8736, DSN 754
email: dexat&e@emh-497ig.bolling.af.mil

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Approval of the Test & Evaluation Policy for DoDIIS Intelligence Mission Applications

1. The Test & Evaluation Policy for DoDIIS Intelligence Mission Applications shall be effective upon review and signature of the below parties. It will be reviewed and updated periodically to coincide with the review and update of the DoDIIS Instructions from which it derives its authority.

2. This document applies to the DExAs and Program Managers and the Community of Test Agencies responsible for developing and testing Intelligence Mission Applications in and for the DoDIIS Community.

3. Individuals wishing to comment on, discuss or provide input to the next revision may do so by contacting the DExA or the DExA representatives at the location on the front cover or by email to dexat&e@emh-497ig.bolling.af.mil

/s/ STEVE D. FAGER
GS-15, Dept of the Air Force
DExA, Test and Evaluation

Date: 5 Mar 1999

EXECUTIVE SUMMARY

This Policy document:

- Fulfills the mandate expressed in Section 4 - DODIIS TESTING AND EVALUATION, of the Department of Defense Intelligence Information System (DoDIIS) Instructions. Specifically, *" . . . to oversee the T&E portion of the DoDIIS IMA Certification Process."* In doing so, this document activates and implements the guidance for Test and Evaluation promulgated in many places throughout the DoDIIS Instructions document approved by the DMB, January 1999.
- Provides guidance to testing agencies responsible for certifying Intelligence Mission Applications for compliance with the OSD directed DoDIIS Common Operating Environment.
- Provides certification process guidance to the Program Managers and DExAs responsible for supervision of Intelligence Mission Application development and testing.
- Provides in a series of Appendices and references, checklists and guides to assist PMs, Testers and application users prepare for testing and post-test milestones.

CHANGES FROM TEST AND EVALUATION POLICY FOR DODIIS AIS,

18 NOV 1997

This list of changes is not totally inclusive, it does however, meet the intent of Action Item (AI) #54 generated at the TPOC of 5-6 February 1998 requesting future changes to the document be highlighted. Highlighting changes was deemed totally impractical given the extensive reformatting and revision to this version of the document. Any specific questions or comments are welcome and may be addressed to the DExA for Test and Evaluation as noted on the front cover.

Status:	**Where:**	**What:**
changed	Title	Automated Information System (AIS) to Intelligence Mission Application (IMA)
FRONT		
added	Front	Memorandum for Distribution
added	Front	Executive Summary
added	Front	Changes from Version of 18 November 1997
SECTION 1 - Background and Introduction		
reformatted	Section 1	Paragraphing
added	Section 1.2	Introduction
added	Section 1	Fig 1-1. Test & Evaluation Process Loop
modify	Figure 1-2	Place JITC Certification in correct context
SECTION 2 - Test and Evaluation Objectives		
		Former Section 2 redesignated Appendix A - References
expanded	All	Topics to cover major milestones in the Certification Process
SECTION 3 - Testing Milestones and Events		
re-titled		"Testing Milestones Activities" to ". . .Events"
converted	This and subsequent Sections	Tables to integrated text. Table entries retained are indicated as an alpha-designated subparagraph. Alpha-designated sub-paragraphs have task-equivalence similar to the diamond-designations "◆" in the DoDIIS Instructions. Alpha-designations are more easily references (i.e. 3.1e)
new	para 3.3	Software Baseline
reformat/revise	para 3.4	Document Review
reformat/revise	para 3.6	JITF Testing
expanded	para 3.6.1, 3.6.2	Integration testing - to include adding categories of integration requirements and conditions (3.6.2) to be met for a successful evaluation.
added	para 3.7	JITF Y2K Testing
added	para 3.8	Independent Verification and Validation Evaluation
revised	para 3.9	JITC Testing - adds definition of ratings
added	para 3.10	JITC Y2K Interoperability Testing
reworked	para 3.11	INFOSEC Testing - added categories of specific findings
added	para 3.12	BETA II testing
add placeholder	para 3.13	DoDIIS Configuration Definitions
SECTION 4 - DoDIIS Test and Evaluation Process Descriptions and Responsibilities		
deleted	from title	*". . .Process* **Oversight** *Descriptions. . ."*
reformat/revise	throughout	topics
reduced	para 4.5 (prev 5.1.2)	VTF. Separate VTF documentation is available from the

		JITF
reduced	para 4.7 (prev 5.1.5)	Testing Configuration Management. Separate CUBIC CM/CMDB documentation is available from the JITF
relocated	to Section 3	data related to JITF, JITC and INFOSEC Findings
deleted		subsection dealing with External Organizations

SECTION 5 - Review and Termination Renumbered from Section 6

APPENDICES

new	A - References (prev Section 2)
new	B - Definition Of Terms
new	C - Acronyms & Abbreviations
revised	D - JTPM Planning Questionnaire (prev Appendix A)
re-designate	E - JTPM Memo (prev Appendix B)
new	F - JTRR Mandatory Agenda Items
revise/expand	G - BETA II Testing Recommendations (prev Appendix C)
revise	H - BETA I & BETA II PMO Security Certification Letter. (prev Appendix D). Revised the Letter to be generic.
rename/revise	I - DoDIIS IMA Version Release Policy (prev Appendix E) Revised release definitions to conform to DoDIIS Instructions
re-designate	J - Training Certification (prev Appendix F)
new	K - Pass/Fail Criteria for JITF Integration Testing
revise	L - Recommendation Criteria (prev Appendix G)
new	M - DoD Year 2000 Compliance Checklist.

TABLE OF CONTENTS

APPENDICES

FIGURES

SECTION 1

BACKGROUND AND INTRODUCTION

1.1 Background. In June 1995, the Unified Commands urgently requested integration, interoperability, security, and training certification of Department of Defense Intelligence Information Systems (DoDIIS) Automated Information Systems (AISs) to ensure fielding of quality software to DoDIIS Sites. In June 1996, the DIA/DR approved the DoDIIS AIS Certification Process for all DoDIIS AISs destined for installation at DoDIIS sites. To focus attention to the Intelligence Community and to prepare for the transition to the Defense Information Infrastructure – Common Operating Environment (DII-COE), AIS applications shared among DoDIIS Sites were re-designated Intelligence Mission Applications in 1998. The DoDIIS Intelligence Mission Application Certification Process is described in the DoDIIS Instructions document, which is updated annually.

The DExA for Test and Evaluation (DExA for T&E) was established to provide oversight to the T&E portion of the DoDIIS IMA Certification Process. The DExA oversees a testing and evaluation approach that includes:

- The Joint Integration Test Facility (JITF): designated integration, compliance, and IV&V authority – responsible for IMA integration evaluation, verifies IMA compliance with the DoDIIS Infrastructure, and performs verification and validation for IMA compliance with the DoDIIS Instructions. Test reports generated from the T&E portion of the Certification Process become part of the Acquisition Decision Memorandum (ADM) as outlined in the DoDIIS Instructions document.
- Information Security (INFOSEC) Certifiers: designated security certification authority for DoDIIS IMAs – responsible for validating Director of Central Intelligence Directive (DCI) 1/16 security requirements.
- The Joint Interoperability Test Command (JITC): designated interoperability authority – conducts interface tests or witnesses remote tests based on where required systems and operators are available. Certifies interoperability requirements have been successfully met.
- Beta II Testing Sites: designated operational deployment assessment authorities – provides facilities and personnel for certification of IMA interoperability and functionality with other IMAs or automated information systems in an operational environment.
- DoDIIS IMA Program Management Offices (PMOs): designated certification authority for functional testing - responsible for quality design, development, project level integration and testing, and delivery of IMAs that satisfy end-user expectations for functionality, performance, security, and training. Responsible for design and preparation of Beta II tests.
- DIA's General Intelligence Training System Division/DAJ-GI, acting for the General Intelligence Training Council (GITC), or Community Intelligence Training Council (CITC) in coordination with the National Imagery and Mapping Agency (NIMA) College – the designated IMA training certification authorities.

1.2 Introduction. The DoDIIS community has emphasized three objectives: interoperability, sharable resources, and modularity of mission applications. DoDIIS began implementation of these objectives in its current infrastructure termed the DoDIIS Client Server Environment. This has been accomplished in part by planned scheduled selection of technology and by sound management.

As the Intelligence Community transitions to the Defense Information Systems Agency (DISA) Defense Information Infrastructure Common Operating Environment (DII-COE), the DoDIIS community shares these objectives as documented in the following:

- *Defense Information Infrastructure (DII) Common Operating Environment (COE) Integration and Runtime Specification (I&RTS)*
- *Defense Information Infrastructure (DII) Common Operating Environment (COE) Baseline Specifications*

The three objectives are also shared across the Intelligence Community, not only because of common goals for integration and interoperability, but also because mission applications and data are in use across the community, not just within a single entity such as DoDIIS. The DoDIIS community has frequently contributed its own technical expertise. The planning and implementation by DoDIIS of the DII-COE architecture will offer common solutions to other Intelligence Community members.

The DISA DII-COE concept has been described as:

- an architecture that is fully compliant with the *DoD Technical Architecture for Information Management (TAFIM), Volumes 2 and 3*, and the *DoD Joint Technical Architecture (JTA)*
- an approach for building and testing interoperable systems
- a collection of reusable fully tested software components
- a software infrastructure for supporting mission area applications
- a set of guidelines and standards

In March 1996, the DoDIIS Management Board (DMB) voted to begin the transition to the DII-COE. The implementation of a fully compliant (i.e., level 8 compliance) DII-COE system will require extensive effort.

1.3 Purpose. The purpose of this document is to provide the following entities with details on specific procedures and responsibilities associated with each step of the IMA Certification process as it applies to Testing and Evaluation (T&E):

- the Test Agencies:
  - the Joint Integration Test Facility (JITF), a component of the Information Handling Branch (IFEB), Information Directorate, Air Force Research Laboratory, Air Force Material Command, at Rome, New York

- the Joint Interoperability Test Command (JITC), a component of the Defense Information Systems Agency, headquartered at Ft. Huachuca, Arizona
- INFOSEC Certifiers, components of the information security organizations within the DIA, Air Force, Navy, and Army

- the Management and User Communities:
  - The DExA for the IMA
  - Program Management Offices (PMOs)
  - Military Services and Unified Command SIMOs
  - BETA II test site personnel
  - DoDIIS Intelligence Mission Application functional users.

The policies in this document describe key responsibilities necessary for the implementation of a successful Certification Process and should aid Program Managers in the development of contract statements of work. A reference is also provided for appropriate testing documentation and information on test agency architectures.

1.4 Scope. The design, implementation and testing of segments does not significantly change the life cycle process for intelligence mission applications as documented in the DoDIIS Instructions and in the DoD 5000-series directives. The T&E aspects as well as most of the other steps in the certification process are fairly constant. Within each step, some activities may be altered particularly due to the transition to DII-COE, DII-COE compliance testing, and the pending inclusion of the IV&V; however, the objectives of each step shall be adhered to.

Figure 1-2 provides a diagram of the mission application life cycle process. The circled areas depict functions found within the Testing Process. The steps in the IMA life cycle process that play important roles are in bold and are discussed later in this document. Note that these steps mesh with the IMA certification process as illustrated in Figure 1-3.

The steps in the life cycle process are defined by the DoDIIS Management Board (DMB) and are executed in coordination with the JITF. The DoDIIS Executive Agent (DExA) for T&E provides management oversight.

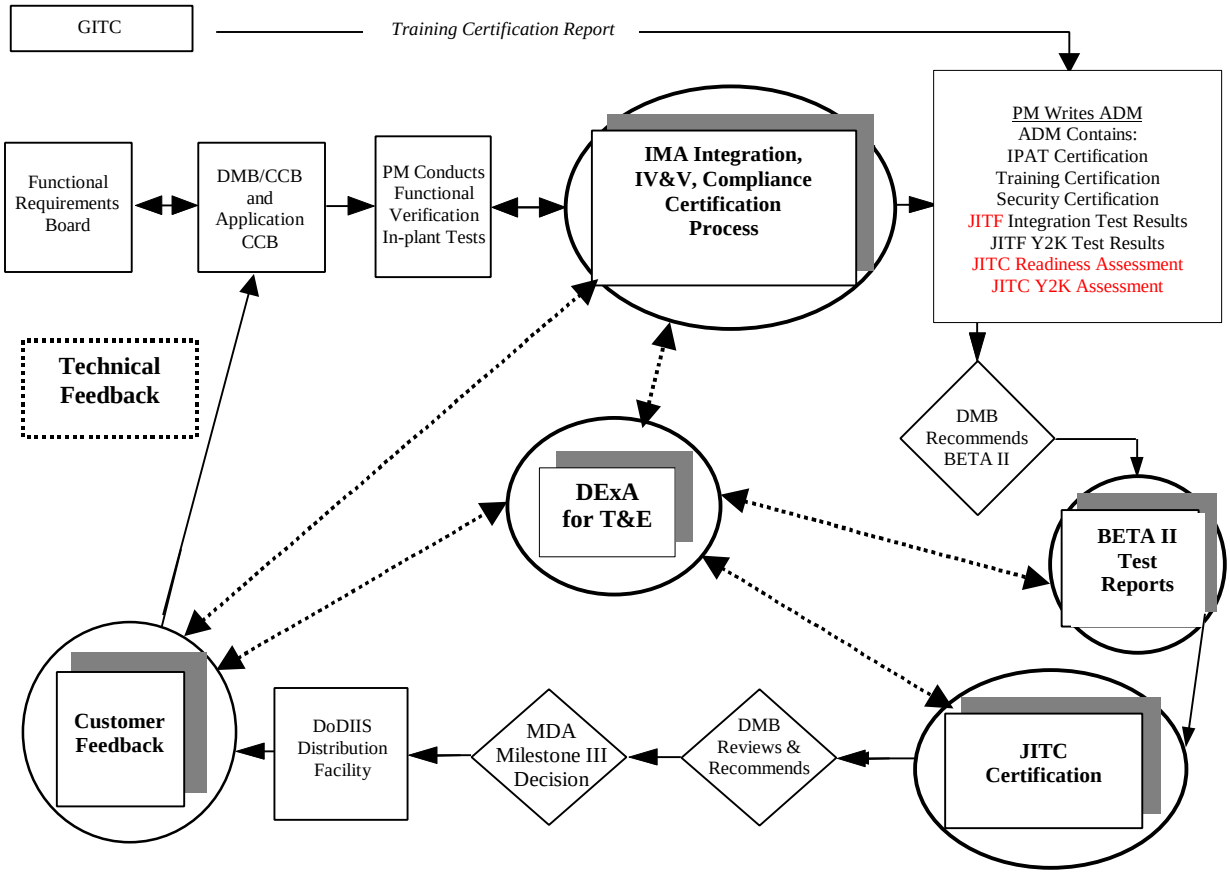

Figure 1-1. T&E Process Loop

The dotted lines in Figure 1-1 indicate feedback points. Expertise, lessons learned, and technology are shared between these functions. There will be technical feedback to PMOs, DoDIIS sites, and the DMB as a result of the certification process. The net result of these feedback loops is to improve the overall process. Improvements will be implemented as updated integration requirements, revised system documentation, enhanced distribution technology, and other products become available.

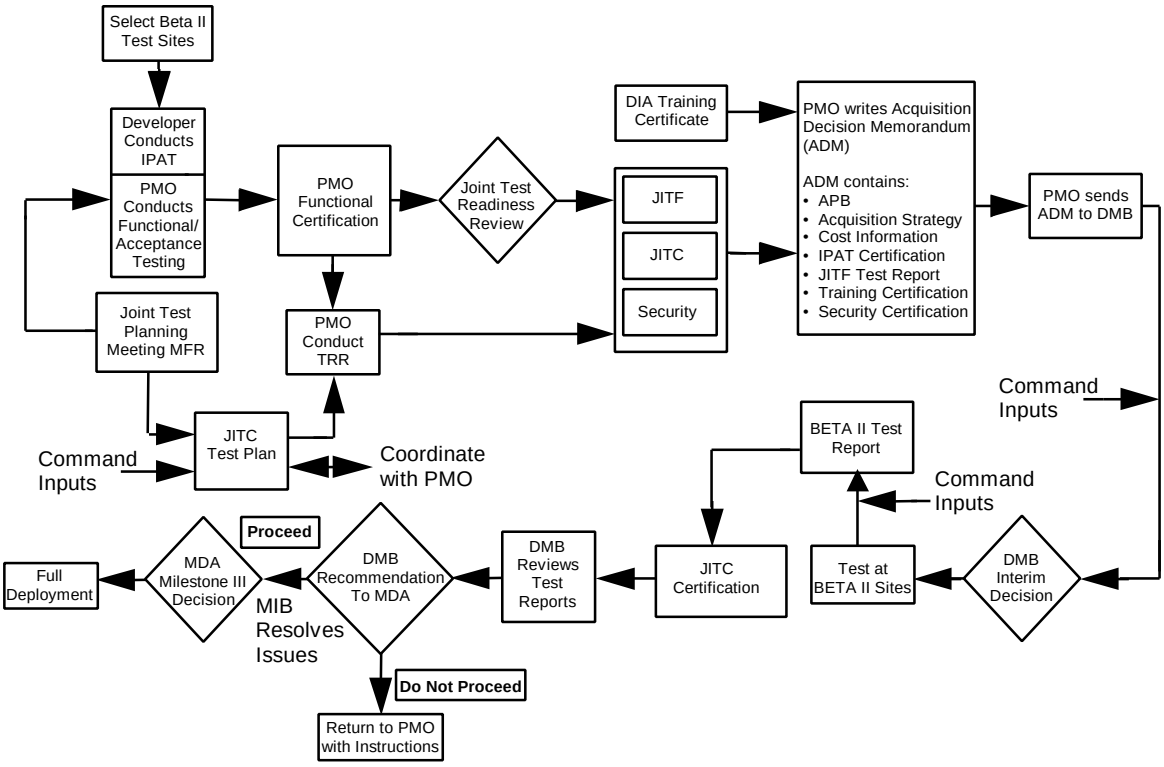

Figure 1-2. The DoDIIS IMA Certification Process

The DExA is supported by the Test Agencies. Prior to DoDIIS IMA certification, the Program Managers for these applications must conduct Configuration Control Boards (CCBs) and User Conferences to plan the release schedules and implementation of application requirements. These activities include implementation of DII-COE compliance and DoDIIS integration compliance requirements, as tasked by the DMB.

The synthesis of integration and compliance testing and the planned IV&V process results in a beneficial arrangement for the DoDIIS community bringing to the certification process the full range of expertise resident with the JITF. The arrangement will also provide a firm foundation for introducing and implementing Configuration Definitions (TBD) as created, as a tested and distributed product**.**

SECTION 2

TEST AND EVALUATION OBJECTIVES

The overall goal of the DoDIIS test and evaluation (T&E) process is to provide data to assess how well an application conforms to standards and operating requirements and to assess the risk of fielding the application. The DoDIIS intelligence mission application T&E process is conducted in accordance with Joint Technical Architecture (JTA) guidance to satisfy the following objectives:
The overall goal of the DoDIIS test and evaluation (T&E) process is to provide data to assess how well an application conforms to standards and operating requirements and to assess the risk of fielding the application. The DoDIIS intelligence mission application T&E process is conducted in accordance with Joint Technical Architecture (JTA) guidance to satisfy the following objectives:

- Ensure a thoroughly planned, understood, documented, comprehensive, and consistent test program to fully test and validate the DoDIIS IMA in support of DMB milestone decisions and user needs. (Sections 3.1 – JTMP)
- Verify and certify the IMA can and does function as defined by User requirements and the IMA has no outstanding test findings that would preclude it from passing with reasonable assurance, JITF, JITC, or INFOSEC testing. (Section 3.2 – IPAT Functional Certification)
- Ensure baseline software is available for the test process. (Section 3.3 – Software Baseline)
- Determine adequacy, completeness and availability of documentation necessary to support a full IMA test cycle. (Section 3.4 – Documentation)
- Review final preparations for the test cycle ensuring all elements required for a successful completion of the testing cycle have been addressed and conflicts resolved. (Section 3.5 – JTRR)
- Determine and document the degree to which IMA software conforms and performs to established standards and integration requirements, providing sufficient detail to allow assessment of the risk of integrating applications into the existing and planned infrastructures and platforms. Determine if the IMA software meets requirements mandated in the DoDIIS Instructions. Identify and document for resolution, instances of duplicate functionality within the IMA as mandated by the DoDIIS Instructions. (Section 3.6 – JITF Testing)
- Determine and document interoperability and interface verification test results, and risk of applications operating within existing and planned infrastructures and interfacing with other IMAs as chartered by the Defense Management Board (DMB). Provide Joint Interoperability Certification for IMAs passing test criteria. (Section 3.9 – JITC Testing)

- Determine and document the ability of an IMA to operate without degrading the security of the existing and planned infrastructures. Validate DCID 1/16 security requirements as applies to IMAs and user operations. (Section 3.11 – INFOSEC Testing)
- Determine, document and certify IMA interoperability and ability to function with other IMAs in an operational environment. (Section 3.12 - Beta II).
- Determine and document integration and ability of IMAs to function and exchange data with other IMAs in a shared Y2K computing environment. (Sections 3.7 and 3.10 – JITF and JITC Y2K Testing)

SECTION 3

TESTING MILESTONES & EVENTS

In order to meet the objectives of the DoDIIS Test & Evaluation certification process, a series of formal activities, internal milestones and events are scheduled. Successful DoDIIS IMA certification requires they all be met where applicable, whenever possible and in the timeframe specified.

3.1 Joint Test Planning Meeting (JTPM). The JTPM is the formal start or entry into the DoDIIS IMA Certification Process. It serves as a forum for stating milestones that must be met in the testing phase. The goals of the JTPM include but are not limited to:

- determining the specific objectives of testing
- determining the schedule of the JITF/JITC/Security/Beta II test activities
- establishing a mutual understanding of the level of software release to be tested
- ensuring all parties have a clear understanding of the certification process and the roles test organizations
- identifying the BETA II test site

The JTPM may be conducted as a meeting or via teleconference. The following items govern coordinating, convening, and follow-up of a JTPM:

a. The PMO shall contact the JITF at least three months (90 days) prior to desired start of testing to schedule a JTPM.

b. The PMO and the JITF Representatives will decide the location, date and time for the JTPM.

c. The JITF and PM shall coordinate with all parties who have an interest in participating in the JTPM in sufficient time to allow scheduling participation.

d. The PMO shall have a representative at the JTPM.

e. The DExA for T&E, or representative, shall chair the JTPM as mediator and assist in resolving issues where necessary.

f. The JITF shall provide a DoDIIS T&E Information Package and use this to facilitate test planning activities. The information package includes:

- JITF Test Procedures and integration requirements
- Work plan, which identifies PMO hardware, software, and personnel requirements
- Required documentation and information
- Self-assessment checklists

h. The JITF Work Plan is provided to the IMA PMO in preparation for or at the JTPM. The PMO shall complete the Work Plan and return it to the JITF no later than 60 days prior to the tentatively scheduled test start date.

i. The scope of testing to be carried out shall be determined.

j. Action Items generated at the JTPM shall be tracked and formally documented utilizing the Common User Baseline for the Intelligence Community (CUBIC) Configuration Management (CM) process in addition to being included in the JTPM MFR.

k. The JITF shall post the JTPM MFR on the VTF.

Issues not resolved to the satisfaction of participants at the JTPM will be negotiated and resolved off line at the lowest possible administrative level. The DExA for T&E, having oversight responsibility for Test and Evaluation shall serve as arbitrator when necessary.

A representative from all interested parties should attend the JTPM. A JTPM scheduled for a previously untested DoDIIS IMA or for one that has undergone major revision should be attended by (in addition to the DExA for T&E, the JITF and the PMO) representatives from:

- the JITC
- the applicable Agency/Service INFOSEC Certification organization
- the IMA functional user* community
- the DoDIIS Systems Integration Management Office (SIMO)
- the DoDIIS Engineering Review Board (ERB)
- the PMO training point of contact

*User Community representatives are encouraged to attend the JTPM to provide insight on how the DoDIIS IMA is to be used on-site and to convey any specific testing requirements.

The DExA for T&E publishes for posting on the VTF, a memo for record (MFR) detailing the JTPM actions, milestones, outstanding issues, and decisions. The format for the MFR is contained in Appendix E.

3.2 In-Plant Acceptance Testing. Functional certification (In-Plant Acceptance Testing – IPAT) is the responsibility of the PMO. The JITF will verify this certification is accomplished prior to the start of integration certification testing. The IMA enters the integration certification test phase upon successful completion of IPAT.

a. The PMO shall certify in writing to the DExA for Test and Evaluation (Electronic mail is acceptable) that the IMA has passed IPAT. The IPAT certification letter shall include:
   - a statement that DoDIIS IMA functionality satisfied the Requirements Definition Documentation and that all required functional capabilities are implemented and tested;

- a statement that DoDIIS IMA functionality satisfied the Requirements Traceability Matrix;
- a listing of interfaces tested;
- an attachment containing the IPAT Test Plan, Procedures, and Report with the outstanding related deficiencies (with deficiency code assigned) and schedule of planned fixes;

b. The PMO shall also certify all IPAT Category 1 and 2 findings are closed and all IPAT Category 3 findings are scheduled for disposition.

3.3 Software Baseline. Delivery to the JITF of the software baseline is a critical point in the certification process.

a. The IMA baseline shall be delivered to the JITF by mail or overnight express no later than 14 days before the scheduled test start date.

b. The software baseline submitted by the PMO to the JITF shall be frozen until all tests are complete.

c. No changes will be made to the baseline during certification testing at the JITF with the exceptions of workarounds for Impact 2 and 3 findings.

d. The workarounds will be documented in the test logs maintained by the JITF and in the JITF Integration Test Report.

3.4 Documentation Review. Setting the document review schedule is a JTPM agenda item. Test Agency review of documentation is critical to a successful certification. The documentation review schedule will be determined during the JTPM.

a. System documentation and information shall be delivered to the JITF no later than 30 days prior to the anticipated test dates.

b. The PMO shall provide the following types of documentation to the JITF.

Document Type	Information Content
Requirements Definition Documentation	Provides written requirements for the IMA
Requirements Traceability Matrix	Traces requirements through program documentation
Security Accreditation Documentation	Provides information in accordance with the DODIIS Developer's Guide for Automated Information Systems (AIS) Security in Intelligence Information Systems, November 1993
Test Plans, Procedures and Test Reports	Provides information as described in IEEEE /EIA Standard 12207
Interface Control Document	Provides detailed information on interfaces between applications
Software Version Description	Provides information regarding the

	software version, including changes and known problems
User Documentation	Users manuals, operator guides
Run Time Interface Document	Provides detailed software configuration information
Configuration and Installation Guide	Provides software installation instructions
Transition Plans	Transition details for software upgrades, database changes, future direction for requirements and design of software application
Open Problem Reports	Required no later than the Joint Readiness Review (JRR)

Documents not on the above list but deemed necessary for testing shall be identified at the JTPM and delivered to the JITF no later than 30 days prior to the start of certification testing.

b. Documents not on the above list but deemed necessary for testing shall be identified in consultation between PMO and the Test Agencies.

c. The PMO shall make available to the Test Agencies within the 30-day time frame specified above, any non-listed documents identified.

3.5 Joint Test Readiness Review (JTRR). The JTRR is to be conducted at least two weeks prior to commencement of JITF testing. The JTRR is a formal review, the purpose of which is to ensure that all elements required for the successful completion of integration, interoperability and security testing have been addressed. The JTRR can be conducted via teleconference. The JTRR can occur concurrently with the IMA Certification Readiness Review (CRR) conducted by the PMO, as these reviews are complementary.
A checklist of mandatory topics to be covered in the JTRR is located at Appendix F.

a. The JTRR will be scheduled to occur approximately two weeks prior to the start of testing.

b. The JTRR MANDATORY AGENDA ITEMS checklist found in Appendix F shall be used as the basis of the JTRR.

c. At the conclusion of the JTRR, the JITF shall provide the DExA for T&E notification (e-mail dexat&e@emh-497ig.bolling.af.mil or FAX is acceptable) that document requirements have or have not been met and, if not, what arrangement has been made to obtain the documentation prior to the test date.

Verification that all required documentation has been provided to the JITF, or that satisfactory arrangement for the JITF to obtain the documentation, is mandatory. Non availability of required documentation may result in cancellation of the scheduled test until the required documentation can be provided to the JITF. In the event of cancellation, the DExA for T&E shall coordinate with the JITF on a new test date.

3.6 JITF Testing. The JITF conducts integration testing in support of the DMB, user sites, and PMOs. JITF testing is normally conducted at the AFRL location in Rome, NY. The JITF provides a test environment that includes access to DoDIIS IMAs and connectivity to Scientific and Technical (S&T) Centers and to operational sites. The JITF also provides hardware, COTS and GOTS found at operational sites. This robust environment allows the JITF to simulate commonly used business practices as identified by DoDIIS users.

Test configuration requirement details to support testing of a specific IMA, can be addressed during the JTPM and finalized at the JTRR.

3.6.1 Integration Testing. Integration testing is the responsibility of the JITF. Integration certification, IV&V (planned), and infrastructure compliance testing are mandated in the DoDIIS Instructions, Section 4.1. A positive evaluation of an IMA during integration certification testing is based in large part on the extent that the IMA meets the integration requirements that are documented in the *DODIIS INTEGRATION REQUIREMENTS and EVALUATION Version 2.0,* published by the JITF. The integration requirements identify technical areas of software installation, configuration, and use that influences the IMA's effects on other applications and on the site operating environment. The integration requirements are organized by category:

- Documentation - These requirements evaluate the content and structure of application documents that the system administrator/installer will rely on to plan the application's resource requirements and to determine the effects of the software on the operational and security architectures of the site.
- Installation and Configuration - These requirements evaluate the application installation process and the steps required to configure the application for use.
- Environment - These requirements evaluate the operating environment established or required by the application when it begins execution and the potential effects of that environment on other applications.
- Operation - These criteria examine aspects of the execution of the application that could affect the execution, configuration, or security of other applications, either on the same hardware platform or on other platforms at the site. Included in this category is how administration of the application integrates into the overall system administration strategy of a site.
- User Interface - These criteria are concerned with the integration of the application with the windowing system of the workstation.
- Security - These objectives identify areas of the design and operation of the application that may affect the site security architecture. These objectives may address areas of system security architecture that are not identified in the application security documentation.

3.6.2 Test Findings. The JITF evaluates the extent to which the IMA meets each requirement. For each requirement that the IMA does not meet, the JITF documents a finding and assesses an impact level or a range of impact levels for that finding. Impact levels are described in Appendix K – JITF Pass/Fail Criteria for Integration Testing.

Not all integration requirements have equal weight. That is, the failure to meet some requirements has more significance than the failure to meet other requirements. In addition, the design of the IMA will also influence the significance of unmet requirements.

A successful evaluation means the IMA has passed integration certification, and the JITF will recommend the IMA proceed to the next step in the IMA certification process. An unsuccessful evaluation means the IMA has failed integration certification, and the JITF will recommend all findings be fixed and possibly retested before proceeding to the next step in the IMA certification process.

A successful evaluation occurs when all of the following items are met by the IMA:

- ITEM 1. – Integration testing documents no Impact 1 findings – One or more Impact 1 findings will result in failure of integration certification for the IMA.
- ITEM 2. – Ease of installation and configuration – The integration requirements that pertain to installation and configuration evaluate the ease and efficiency of installing the IMA. The installation and configuration process must proceed smoothly and not require successive restarts or additional, undocumented manual effort. The quality of the installation and configuration documentation is an important factor in determining the ease of installation. The length of time to install the IMA is a critical factor. An efficient installation must be measured in hours rather than days. The JITF test teams critically evaluate the length of time needed to install a mission IMA and estimate the level of effort required to install the IMA at sites with large numbers of platforms or with less experienced system administrators. The target threshold for installation and configuration for the IMA server software is 20 working hours. Installation and configuration covers all activities required up to initial data load and/or operation of the software. Client installation should require no more than two hours to complete.
- ITEM 3. – Support for target operating systems – The *DODIIS Instructions* specify the target operating systems and versions that IMAs must support in the DODIIS community. An IMA must support at least one of the target operating systems specified in the *DODIIS Instructions*. The IMA must operate on versions of the target operating system currently fielded in the DODIIS community rather than moving ahead to a newer version that may not be fielded at the majority of sites or lagging behind on older versions that DODIIS sites have already abandoned. Since there are frequently issues of operating system patches that are required to maintain stable operating environments, the JITF has specified integration requirements that emphasize IMA documentation must clearly identify the operating system patches needed to install and operate the IMA.

- ITEM 4. – Sixty percent of integration requirements are met – The goal of integration certification testing is to evaluate the capability of an IMA to integrate and operate successfully in the DODIIS environment. The consequence to integration and operation of an unmet requirement will depend in great part on the design and configuration of the IMA. The JITF test teams carefully evaluate each finding to determine the appropriate Impact level. While no hard and fast percentile of requirements met can be established for all IMAs, an IMA should pass, as a minimum, 60 percent of the integration requirements. Passing fewer than 60 percent will mean too many Impact 2 and 3 findings have accumulated; this accumulation will indicate the level of effort to integrate the IMA is unacceptably high.
- ITEM 5. - Capability to operate on shared data server **TBD**

Integration requirements are published by the JITF in *The DoDIIS Integration Requirements and Evaluation, Version 2.0* and may be viewed on the VTF at Intelink http://web1.rome.ic.gov/jitf or on the Internet at http://www.if.afrl.af.mil/programs/jitf/

3.6.3 Generation and Distribution of Findings. JITF Test Reports document a complete set of findings, open issues, software problems, and documentation errors generated during the test process. These findings are documented under the CUBIC CM process.

a. The JITF shall provide a draft version of test reports to the PMO and the DExA for T&E for comments five working days after completion of JITF testing. The PMO and DExA have 2 days to review and comment on the report from the date received.
b. Written comments on the draft version of the test report shall be submitted to the JITF using the CUBIC CM process available in the VTF.
c. The JITF shall distribute the final test report to the DExA for T&E, DMB, SIMO, ERB, and PMO ten working days after completion of JITF testing.
d. The JITF shall post the final test report on the VTF after release to the PMO.

The final report shall contain a recommendation to proceed to certification based on the criteria set forth in Appendix K and based in large part on the extent the IMA meets the integration requirements documented in the *DODIIS INTEGRATION REQUIREMENTS and EVALUATION Version 2.0*.

3.7 JITF Y2K Testing. The Joint Integration Test Facility (JITF) Test Plan and Procedures identify Department of Defense Intelligence Information Systems (DoDIIS) integration requirements and evaluation methods to be used for Year 2000 (Y2K) testing. This plan includes the evaluation procedures used by the JITF to determine the ability of DoDIIS software applications to function in the shared Y2K computing environment without adversely affecting other systems simultaneously operating. It also provides mission application program managers and developers a description of the criteria on which the JITF will base Y2K evaluation.

In support of the test effort, Program Management Offices (PMOs) are responsible for providing installation verification procedures, functional Y2K test procedures, and Y2K data to be used during the JITF Y2K evaluation.

The Y2K Joint Integration Test Facility (JITF) Test Plan and Procedures and test reports are available on the VTF at Intelink http://web1.rome.ic.gov/jitf or on the Internet at http://www.if.afrl.af.mil/programs/jitf/

3.8 Independent Verification and Validation Evaluation. Independent verification and validation (IV&V) testing philosophy and procedures as mandated by the DoDIIS Instructions are being formulated, and are expected to be in effect by the close of FY 1999. Implementation and the process employed by the JITF will be published and made available on the VTF.

3.9 JITC Testing. The JITC, a component of DISA, is responsible for Interoperability Certification testing. DoDD 4630.5 (Appendix A, Reference #18) states the requirement for DoD C4I AIS interoperability. CJCSI 6212.01A (Appendix A, Reference #6) establishes the Defense Information Systems Agency as the responsible agency for interoperability certification. The JITC performs interoperability certification testing of DoDIIS IMAs as chartered by the DMB. The JITC conducts interface tests based on where required systems and operators are available, mainly at the JITF and at BETA II facilities. The JITC may also witness various remote tests conducted by other organizations or by using JWICS connectivity.

Interoperability refers to the ability of two intelligence mission applications or intelligence segments to exchange data:

- with no loss of precision or other attributes
- in an unambiguous manner
- in a format understood by both applications
- where the interpretation of the data is precisely the same

The JITC produces and publishes a specific test plan for each system based on the results of the JTPM no later than two weeks before the scheduled test.

3.9.1 Interoperability Test Execution. The JITC conducts interoperability testing for the DoDIIS IMAs. This level of testing verifies required interfaces as defined by Interface Control Documents (ICDs) and other system documentation as referenced in the *Interoperability Certification Test Program Plan for the Department of Defense Intelligence Information Systems (DoDIIS) Migration Systems*. JITC Certification requires that a detailed review of system documentation be conducted to determine interoperability requirements and to identify any standards or criteria for exchange of information that can be gathered from the documentation.

3.9.2 Interoperability Test Certification. The JITC tests and certifies the ability of a tested application to interface with other systems (reference: JITC Program Management Plan). The JITC Certification is for a system-to-system interface and includes the

equipment string, software configuration, and operating environment of the systems under test. DoDIIS IMAs perform numerous functions involving an exchange of data. Each exchange function is tested to determine if information can be exchanged in the manner it was designed and in a manner useful to the intelligence analyst or user. In addition, this testing identifies resource/standardization conflicts and operational impacts. JITC uses the following interoperability definitions in assigning ratings to the interfaces under test:

C-1. System meets ALL joint interoperability requirements that are defined by the users.

C-2. System meets SOME of the joint interoperability requirements that are defined by the users and the unmet requirements have resulted in MINOR operational impacts.

C-3. System meets SOME of the joint interoperability requirements that are defined by the users and the unmet requirements have resulted in MODERATE operational impacts.

C-4. System meets SOME of the joint interoperability requirements that are defined by the users and the unmet requirements have resulted in SIGNIFICANT operational impacts.

C-5. System does not meet joint interoperability requirements that are defined by the users.

3.9.3 Generation and Distribution of Findings. The information generated by the JITC testing process is documented utilizing a Joint Interoperability Certification (JIC) Letter and a Test Report, which present the JITC's findings on DoDIIS IMA interoperability status. Joint Interoperability Certifications and Test Reports are generated following the completion of BETA II. Following Beta I, JITC will provide the PMO and DMB an assessment of the IMA's readiness to proceed to Beta II. The Recommendation to Proceed criteria is found at Appendix L. These findings will be documented under the CUBIC CM process.

a. The JITC shall provide a draft version of the Joint Interoperability Certification to the PMO and the DExA for T&E for comments seven working days after completion of JITC Beta II testing.

b. The JITC shall provide a draft version of the JITC Test Report to the PMO and the DExA for T&E for comments 14 days after completion of JITC BETA II testing.

c. The JITC shall distribute the Joint Interoperability Certification and Final Test Report to the DExA for T&E, the DMB, SIMO, ERB, and the PMO not more than 30 days after completion of JITC BETA II testing.

d. The JITC shall include in the Joint Interoperability Certification and Final Test Report a recommendation to proceed/not to proceed to the next phase fielding in accordance with the DoDIIS IMA Certification Process.

The JITC will provide the final test report to be posted on the VTF ten days after release.

3.10 JITC Y2K Interoperability Testing. The DMB also directed that all DODIIS intelligence mission applications (IMAs) be Year 2000 (Y2K) tested for the exchange of data in a Y2K environment, and that JITC include Y2K testing in their existing test procedures. Due to the potentially "destructive" nature of Y2K testing, DODIIS Y2K interoperability testing can only be performed in a laboratory environment, such as at the JITF. Therefore, the JITC, as part of its Beta I testing, will conduct Y2K interoperability testing at the JITF. Only those IMAs that pass JITF Y2K integration testing will be tested by JITC for interoperability in a Y2K environment.

3.10.1 JITC Test Support. The JITF will provide Y2K Integration test results, including test data, to the JITC for use in Y2K interoperability tests. Based on the successful completion of JITF Y2K Integration testing, the JITC will proceed to Y2K Interoperability testing.

The JITF will install the IMA's interoperability interfaces to be tested on the JITF Y2K test network. JITC will conduct a Y2K interoperability test using this network assisted by JITF Test Engineers.

If the interoperability interfaces for the IMA under test are not available at the JITF, the JITC will coordinate with the PMO for a suitable test location.

3.10.2 Generation and Distribution of Findings. Test results from both JITF and JITC testing will be analyzed by JITC. A JITC Y2K Assessment Letter will be generated within seven days of completion of Y2K interoperability testing. This letter is separate from the Beta II readiness assessment and Joint Interoperability Certification letter. The results of the Y2K interoperability test will also be included in the JITC Interoperability Test report following completion of Beta II. If no Beta II testing is required then a separate Y2K interoperability test report will be prepared.

3.11 INFOSEC Testing. INFOSEC Certifiers include DIA, Air Force, Army, and Navy Security representatives. Security Certifiers are responsible for validating Director of Central Intelligence Directive (DCID) 1/16 security requirements IAW Mode of Operation, testing interoperability with the DoDIIS infrastructure, validating Security Concept of Operations (SECONOPS) and testing user efficiency/training as it relates to security.

3.11.1. INFOSEC Test Architecture. All security testing will be completed on the specific DoDIIS IMA suite of equipment installed at the JITF or BETA II sites. In addition, INFOSEC testing may also occur at the PMO/Contractor site.

3.11.2. INFOSEC Test Execution. Every DoDIIS IMA must undergo Security Certification. The system must be tested to determine the adequacy of its security features. It must be evaluated against the criteria of DCID 1/16, DIAM 50-4, and DoDD 5200.28. System accreditation documents (CONOPS, security architecture, security requirements, design analysis, test plan, and test procedures) must be reviewed. The functionality of the security design must be tested to ensure all features work as

accurately and completely as intended. The security testing is usually conducted in conjunction with testing at the JITF and at the BETA II site.

a. INFOSEC Certifiers shall test the following:

- System Discretionary Access Controls
- Audit Capabilities
- User ID/Authentication
- Data Integrity
- System Integrity
- Data Labeling

b. The INFOSEC Certifiers shall identify findings or discrepancies broken down by level of possible impact on the site security baseline as described below.

Categories of specific findings are:

- CATEGORY I – A significant security finding which must be fixed before a site or site component can go operational or must be corrected before an operational site or site component can continue operation.
- CATEGORY II – A security related finding which must be fixed within a specific time period (i.e., 4 months) in order for approval to be granted.
- CATEGORY III – A security relevant recommendation for which implementation is a command option.
- CATEGORY IV – A non-security relevant recommendation for which implementation is a command option.

3.11.3 Generation and Distribution of Findings The information generated by the Security Certification testing process is documented in the BETA I and BETA II PMO Security Certification Letter (Appendix H) and the Security Test Report. Both these documents contain the Security Certifier's recommendation on IMA security status.

a. The PMO shall present the Security Certification Letter to the BETA II site Information System Security Manager (ISSM) before BETA II testing can begin.

b. The INFOSEC Certifiers shall include a complete set of findings, open issues, software problems, and documentation errors within the Security Test Report.

The test report is distributed to the DExA for T&E, PMO and ISSO/ISSM not more than seven days after completion of security testing. The Security Certifier will provide the test report on VTF, Intelink http://web1.rome.ic.gov/jitf, ten days after release to the PMO.

3.12 BETA II Testing. The principle purpose for BETA II testing is to certify IMA interoperability and functionality with other IMAs or automated information systems in

an operational environment. Since the BETA II testing environment most closely represents an operational environment, it is considered the primary testing event for interoperability certification. The PMO is charged with the responsibility for preparations for the BETA II test. The principle objectives of Beta II are to:

- validate that the IMA works in an operational environment
- ensure problems encountered during BETA I are cleared
- verify IMA INFOSEC functions in an operational environment

a. Prior to BETA II, the PMO shall provide to the appropriate Test Agency, a Test Plan detailing critical operational and performance issues and criteria that defines success. The criteria should be quantitative or qualitative and detail what must be met to achieve operational effectiveness.

b. The BETA II test site shall provide a written report of the BETA II test results to the other Test Agencies, DExA for T&E, DoDIIS SIMO, and ERB.

3.12.1 BETA II Preparations. As part of the preparations for BETA II Testing, the:

a. PMO shall identify the BETA II test site prior to the JTPM. Guidelines for BETA II test site selection are provided in Appendix G.

b. PMO shall be responsible for IMA software installation at the BETA II site

c. The IMA shall be installed at the Beta II site by following the installation plan published by the PMO and validated at the JITF

d. PMO shall provide test procedures for verifying the functionality of the system.

e. BETA II Site personnel shall develop operational scenario testing procedures based on anticipated operational use of the application

3.12.2 BETA II Responsibilities. A representative from the BETA II test site is encouraged to attend the JTPM and participate in all formal test activities to include IPAT and BETA I testing. The format to be used for BETA II test results is provided in Appendix G.

To ensure successful BETA II testing, participant responsibilities are:

a. the BETA II Site shall document the results of the BETA II test

b. the BETA II Site shall provide test results to the DMB for use in the MDA III decision within two weeks after test completion.

c. the PMO and JITC shall coordinate activities coincident to interoperability testing at the BETA II Site

d. the JITC shall plan interoperability events to be conducted at the BETA II

e. the JITC shall collect interoperability data from the BETA II site and identify interoperability shortfalls

f. the JITC and INFOSEC security certifier will also conduct necessary testing to complete test objectives identified during the JTPM
g. the JITC shall, upon successful completion of the BETA II, produce a Joint Interoperability Certification memorandum (combining the results from both BETA I and II testing) for the DMB's final fielding decision.
h. the JITC shall, upon successful completion of the BETA II, produce a detailed test report
i. the JITF, on a case by case basis, will attend BETA II to confirm BETA I results and provide support

3.13 DoDIIS Configuration Definition. Configuration Definitions have not yet been defined by the DoDIIS ERB. Creation and implementation are expected to be completed by the close of FY1999.

SECTION 4

DoDIIS TEST & EVALUATION PROCESS DESCRIPTIONS AND RESPONSIBILITIES

4.1 DoDIIS Executive Agent (DExA) for Test & Evaluation (T&E). The DExA for T&E is responsible for managing and/or overseeing the DoDIIS T&E Program as chartered by the DoDIIS Management Board (DMB). The DExA is committed to improving the quality and usability of DoDIIS IMAs in support of the Unified and Specified (U&S) Commands. Specifically, the DExA is responsible for:

a. Defining test requirements and policies to DoDIIS Test Agencies in accordance with DMB directions and user needs.

b. Recommending and coordinating all changes to the DoDIIS T&E Process as they appear in the DoDIIS Instructions, relevant JITF documents and the T&E Policy Document for DoDIIS IMAs. The implementation date for all accepted changes is that expressed as the effectivity date of each individual document.

c. Preparation and advocacy of the DoDIIS T&E budget.

d. Serving as Chair/host for Joint Test Planning Meetings (JTPMs) and determining PMO readiness to proceed to test by the time of the Joint Test Readiness Review (JTRR).

e. Participating in all DoDIIS meetings related to JITF Test and Evaluation.

f. Acting as the primary interface between DoDIIS and the Test Agencies.

g. Acting as a liaison between Test Agencies (to include security and training) and other organizations to mediate concerns and/or issues.

h. Supporting Test Agencies in preparation, coordination, evaluation, and distribution of test results, as required.

i. Monitoring, documenting and implementing corrective measures to improve the overall DoDIIS IMA Certification Test Process.

j. Serving as the Test Process Oversight Committee (TPOC) chairperson.

k. Monitoring the JITF/JITC recommendations to proceed/not proceed to the next phase of testing or fielding in accordance with the DoDIIS IMA Certification Process as presented in this document.

l. Ensuring all testing related deficiencies discovered during the testing process are reported, tracked, and acted on in a timely manner.

4.2 Document and Report Requirements. The DExA produces reports to include:

- JTPM Memos
- T&E Budget Documents

- Annual Report on DExA T&E activities

4.3 Test Process Oversight Committee (TPOC). The objective of the DoDIIS TPOC, as defined in the TPOC Charter, is to provide a forum for test planning to ensure an adequate, comprehensive, and consistent test program to fully validate DoDIIS IMAs in support of DMB milestone decisions and user needs. Specifically, the DoDIIS TPOC objectives are to:

a. Define and document DoDIIS IMA technical issues for JITF Integration, JITC Interoperability, Security, Training, and other DoDIIS testing.

b. Define and document DoDIIS IMA Certification Testing Process issues. Primary areas of concern include, but are not limited to:

   - Test requirements and issues concerning the DoDIIS Common Operating Environment (COE)
   - Year 2000 (Y2K)
   - Distributed integration and interoperability testing
   - Site business practice concerns such as user interfaces, application interfaces, and low bandwidth assessments

c. Support Test Agencies in test plan/work plan review and test results, as required.

d. Address DoDIIS community test issues.

4.4 Test Metrics. The DExA for T&E is responsible for monitoring the overall T&E Process to ensure final user or operator satisfaction with DoDIIS IMAs. To accomplish this, the DExA for T&E has implemented performance-based and results-based management practices in conjunction with the Information Technology Management Reform Act (ITMRA) of 1996.

4.5 Virtual Test Folder (VTF). The VTF is provided to make available to the DoDIIS Community, IMA test reports, Memos For Record (minutes) of JTPMs, TPOCs, and other test related information.

The VTF is administered by the JTIF under oversight of the DExA for T&E. It is the responsibility of the JTIF to make available on-line as soon as possible after receipt, all documents, reports and other items.

Information about the VTF may be obtained by accessing the VTF on the Internet http://www.if.afrl.af.mil/programs/jitf/ or Intelink http://web1.rome.ic.gov/jitf/vtf.html

4.6 Distributed Testing Network (DTN). The DExA for T&E encourages use of the Distributed Testing Network as a means of conserving resources by using connectivity provided by the Joint Worldwide Intelligence Communication System (JWICS) or collateral networks, where available. When warranted, testing may occur utilizing the DTN. Particulars between all parties shall be reached and agreed at the JTPM. The DTN

CONOPS is available through the Internet http://www.if.afrl.af.mil/programs/jitf/ or Intelink http://web1.rome.ic.gov/jitf/vtf.html.

4.7 Testing Configuration Management. The T&E Policy for Configuration Management is summarized in the following.

a. The existing CUBIC CM process shall support the testing CM requirements and shall be the central repository for submitted test findings including software and document test findings and action items (AIs).

b. All test findings written during the testing process by the JITF, JITC, the Security or Training Certifiers, and other agencies shall be identified and tracked.

c. CM shall support submittal, evaluation, approval or disapproval, implementation, verification, and release according to established procedures.

The CUBIC CM repository and further information about it is available through the Internet http://www.if.afrl.af.mil/programs/jitf/ or Intelink http://web1.rome.ic.gov/jitf/vtf.html.

4.8 Test Organizations

4.8.1 Joint Integration Test Facility (JITF). The JITF evaluates the capability of software applications to operate in an environment in which computing resources including processors, configuration files, networking facilities, and administration facilities are shared by many applications rather than reserved by one system for its exclusive use. Evaluation methods include inspection, analysis, demonstration, and testing. The JITF provides support to DoDIIS throughout the life cycle of DoDIIS IMA and integration in the following areas:

a. Reviews all DoDIIS application life cycle documents and provides comments to originators, as required.

b. Provides written notification to DExA for T&E after the JTRR of system documentation status IAW Section 3.3.c of this document. Notification may be by email dexat&e@emh-497ig.bolling.af.mil, FAX or Memo.

c. Performs Installation/De-installation verification.

d. Performs DoDIIS Infrastructure Compliance Testing, including DII COE application compliance.

e. Performs testing in accordance with the *DoDIIS Year 2000 Concept of Operations for Integration and Interoperability.*

f. Supports testing at user sites and joint interoperability testing, as required.

g. Supports system security certification.

h. Provides lessons learned or other assistance to DoDIIS PMOs and developers as needed or requested.

i. Verifies functionality of, and identifies any duplicate functionality in, DoDIIS IMAs, as tasked by the DMB, during PMO In-Plant Acceptance Tests (IPAT) (TBD) or Functional Acceptance Testing (TBD).

j. Provides technical support and information to user sites as required.

k. Provides a JITF Distributed Testing Network (DTN) for integration testing.

l. Under the oversight of the DExA for T&E, the JITF shall also

- be responsible for reviewing and taking action to retest (if necessary) all other DoDIIS IMA deficiencies reported by DoDIIS users that may have been missed during the testing cycle
- The JITF shall also advise the DExA for T&E of any instances of requests from DoDIIS Users for DoDIIS IMA deficiency investigation or retest. Notification may be through electronic means (e-mail dexat&e@emh-497ig.bolling.af.mil or FAX) or by memo.
- Review minor and maintenance releases to determine the need for testing, and provide a go/no go recommendation to the DMB Secretariat concerning readiness to field.

JITF information may be accessed through their INTELINK home page at http://web1.rome.ic.gov/jitf. Selected information may be accessed through JITF's Internet site at http://www.if.afrl.af.mil/programs/jitf/.

4.8.2 Joint Interoperability Test Command (JITC). Interoperability consists of determining the ability of a system to provide and receive services from other systems and the ability to use the services to operate effectively. Interoperability is the condition achieved when information or services can be exchanged directly and satisfactorily between systems and/or system users. The JITC provides support to DoDIIS throughout the life cycle of DoDIIS IMAs and interfaces in the following areas:

a. Assists the DoDIIS community in identifying interoperability requirements and criteria.

b. Identifies the required interfaces at the JTPM.

c. Indicates those interfaces they plan to test and provides justification for required interfaces that cannot be tested.

d. Certifies required system interfaces, communications paths, and functions as interoperable with other DoDIIS IMAs.

e. Reviews all life-cycle documents associated by DoDIIS applications and provides comments to originators, as required.

f. Performs standards profile testing and standards conformance testing, to include Y2K interoperability testing in accordance with the *DoDIIS Year 2000 Concept of Operations for Integration and Interoperability.*

4.8.3 INFOSEC Certifiers. The INFOSEC Certifiers are from the security offices of the DIA, Air Force, Army, and Navy. Under the site-based accreditation methodology, a simplified structure and line of responsibility is established. DIA, as the Principal Accreditation Authority (PAA), working through the Service Certifying Organizations

(SCO) (Army, Navy, or Air Force) and the Site Information Systems Security Officers/Managers (ISSOs/ISSMs), provides final certification of a specified system. The SCO's specific responsibilities include:

a. Reviewing all life cycle documents associated with applications and commenting as required.

b. Providing security, technical, and policy guidance to requesting parties.

c. Performing security testing and evaluations on new or modified DoDIIS IMAs in accordance with appropriate security requirements.

d. Granting interim authority to operate for DoDIIS IMAs pending final decision by the Director, DIA.

e. Providing certification recommendations to DIA for those systems and sites under their purview.

4.8.4 Program Management Offices (PMOs) Responsibilities. DoDIIS IMA PMOs are responsible for the following:

a. Complying with the requirements of the DoDIIS IMA Certification Process.

b. Providing an Interoperability Certification Test Program Plan for DoDIIS IMAs, and the Joint Integration Test Facility (JITF) Test Procedures: Volume 1 - Infrastructure Compliance Testing, Volume 2 - Installation and Integration Scenario testing

c. Complying with the DMB-directed DoDIIS IMA Version Release Policy in Appendix I of this document.

d. Selecting BETA II site(s) according to selection criteria listed in Appendix G of this document.

e. Scheduling the JTPM with the JITF. (At this time, the PMO should have selected a BETA II site and notified the Site personnel of the scheduled JTPM.)

f. Participating in the JTPM.

g. Distributing all base-lined application documents to JITF/JITC for comment NLT 30 days prior to the scheduled test. See Section 3.4 – ***Documentation Review*** - for requirements. If required documentation is not provided, the scheduled test will be cancelled until documentation can be produced. New test dates will be decided by the DExA for T&E in consultation with the JITF

h. Completing the Interface Control Document using the Interface Requirement Specification (IRS) in MIL-STD 498[1], DID Number DI-IPSC-81434 as the standard format.

i. Completing a configuration and installation guide using the Software Installation Plan (SIP) in MIL-STD 498, DID Number DI-IPSC-81428 as the standard format.

j. Subscribing to or linking to the Virtual Test Folder (VTF).

[1] MIL-STD 498 was cancelled effective 27 May 98; however, the DIDs remain in effect.

k. Inviting Test Agencies to witness In-Plant Acceptance Testing (IPAT) conducted by the developer.

l. Conducting functional testing.

m. Submitting an IPAT Functional Certification Letter to JITF/JITC according to requirements in Section 3.2 of this document.

n. Submitting the PMO's operational application baseline for JITF Integration Testing, JITC Interoperability Testing, Security Certification, and Training Certification. All required functional capability must be implemented in the baseline. Also, the delivered baseline must not contain any problems considered cause for failure, or receiving a recommendation not to proceed with certification, i.e. the severest rating applied by any of the test agencies. Problems considered limitations to proceeding with certification must have workarounds or be resolvable.

o. Preparing and sending an Acquisition Decision Memorandum (ADM) to the DoDIIS SIMO office in accordance with the DoDIIS Instructions and DIA Regulation 65-13.

p. Submitting the PMO Security Certification Letter to the Beta II site ISSM/ISSO, prior to the Beta II test. (Appendix H)

q. Coordinating BETA II testing at an operational site with the ISSO/ISSM and SIMO.

r. Coordinating system developer support at BETA II testing, if necessary.

s. Updating the ADM after BETA II testing.

t. Prior to BETA II, the PMO will be required to provide a Test Plan that will detail critical operational and performance issues and criteria that define success. The criteria should be quantitative or qualitative that must be met to achieve operational effectiveness.

u. Validating the implementation or approval of changes to the baseline based on BETA II findings with BETA II representative participation/coordination.

SECTION 5

Review and Termination. The roles and missions of the DoDIIS T&E process described in this guidance document will be reviewed annually by the DExA for T&E. CUBIC CM (http://www.if.afrl.af.mil/programs/cm/) maintains points of contact for DoDIIS IMAs and T&E management organizations. Recommendations and changes to this document may be submitted at anytime by written notice in DRR format. This guidance document will remain valid until terminated or superseded by the DExA for T&E. The DExA for T&E will set implementation dates for all changes to the T&E process not later than 30 days after publication unless otherwise directed.

APPENDIX A

REFERENCES

The following list of references is not an exhaustive bibliography but is intended to provide the basis on which the discussions rely. The listing covers the main text and the Appendices.

1. Secretary of Defense memorandum, subject: Year 2000 Compliance, 7 August 1998
2. Deputy Secretary of Defense memorandum, subject: Year 2000 (Y2K) Verification of National Security Capabilities, 24 August 1998
3. Office of the Assistant Secretary of Defense (C3I) memorandum, subject: Year 2000 (Y2K) Compliance – FY 1999 Reporting Requirements, 23 September 1998
4. ASD (C3I) Memorandum, Subject: Year 2000 (Y2K) Refined Reporting Requirements for DoD, March 1997
5. ASD (C3I), Department of Defense Year 2000 Management Plan, Version 1.0, April 1997 – *(a Version 2.0 DoD Y2K Mgmt Plan, in "For Signature Draft" form, is currently in coordination at DoD.)*
6. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01A, Compatibility, Interoperability, and Integration of Command, Control, Communications, Computers, and Intelligence Systems, 30 June 1995
7. Director of Central Intelligence Directive (DCID) 1/16, "Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks", July 1988 (SECRET)
8. DIA/DS memorandum, U-634/SYA-2, subject: Year 2000 Federal Acquisition Guidance, March 1997
9. Defense Intelligence Agency Manual (DIAM) 50-4, Department of Defense Intelligence Information System (DoDIIS) Information Systems Security (INFOSEC) Program, 30 April 1997
10. Defense Intelligence Agency Regulation 24-11, General Intelligence Training System (GITS)
11. Defense Intelligence Agency Regulation 65-13, Automated Information System Life Cycle Management
12. Defense Intelligence Agency, DII COE Security Software Requirements Specification (SRS), Version 3.1, 31 October 1997
13. DIA Y2K PMO, DIA Year 2000 Activities Presentation, by Mr. Peter Freed, May 1997

14. Defense Information Systems Agency (DISA), Defense Information Infrastructure (DII) Common Operating Environment (COE) How To Segment Guide, Version 4.0, 30 December 1996
15. Defense Information Systems Agency (DISA), Defense Information Infrastructure (DII) Common Operating Environment (COE) Integration and Runtime Specification (I&RTS), Version 3.1, October 1998
16. Defense Information Systems Agency (DISA), Defense Information Infrastructure (DII) Common Operating Environment (COE) Version 3.1 Baseline Specifications**,** 29 April 1997
17. Department of Defense (DoD) Directive 3305.2, "DoD General Intelligence Training", 20 July 1984
18. Department of Defense (DOD) Directive 4630.5, "Compatibility, Interoperability and Integration of Command, Control, Communications, and Intelligence (C3I) Systems", 12 November 1992
19. Department of Defense (DoD) Directive 5000.1, "Defense Acquisition", 15 March 1996
20. Department of Defense (DoD) 5000.2-R, "Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs"
21. Department of Defense (DoD) Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)", 21 March 1988
22. Department of Defense (DoD) Directive 8320.1, "DoD Data Administration", 26 September 1991
23. Department of Defense (DoD) Joint Technical Architecture (JTA), Version 2.0, 26 May 1998
24. Department of Defense (DoD) Technical Architecture Framework for Information Management, Version 3.0, 30 April 1996
25. Department of Defense Intelligence Information System (DoDIIS) Site Certifier's Guide, SC-2610-143-93, November 1993
26. Department of Defense Intelligence Information System (DoDIIS) Security Architecture Guidance and Directions
27. DoDIIS Developer's Guide for Automated Information Systems (AIS) Security in Intelligence Information Systems, November 1993
28. DoDIIS Instructions, January 1999
29. DoDIIS T&E Information Package
30. DoDIIS Test Process Oversight Committee (TPOC) Charter, 18 November 1996 - *(in JITF Homepage)*; 13 February 1997
31. DoDIIS Year 2000 Concept of Operations for Integration and Interoperability
32. GAO, Year 2000 Computing Crisis: An Assessment Guide, Exposure Draft, February 1997
33. Intelligence Community Y2K Conference, EDS briefing: Year 2000 Test, Validate, Implement, November 1996

34. DoDIIS Integration Requirements and Evaluation, Version 2.0
35. Joint Integration Test Facility RL/IRDO/JITF, Concept of Operations for the DoDIIS Joint Integration Test Facility (DoDIIS JITF) at Rome Laboratory, April 1996
36. Joint Interoperability Test Command (JITC), Interoperability Certification Test Program Plan for the Department of Defense Intelligence Information Systems (DoDIIS) Migration Systems, Version 1.0, August 1996
37. Memorandum of Agreement Between the Joint Interoperability Test Command (JITC), the DoD Intelligence Information Systems (DoDIIS) Management Board (DMB), the DoDIIS Executive Agent (DExA) for Migration Systems Test, and the DoDIIS Joint Integration Test Facility (JITF); "Interoperability Test and Certification of DoDIIS Migration Systems", 19 November 1995
38. Joint Integration Test Facility/Joint Interoperability Test Center/DoDIIS Management Board Memorandum of Understanding (October 1995)
39. Justification and Remarks for Joint Integration Test Facility, Joseph D. Baldino, Chief, Systems Analysis, DIA, Washington DC, (15 June 1995)
40. MIL-STD-498, Software Development and Documentation *(superceded) (DIDs still operative)*
41. OSAF, DC/AQ/ message 211700Z Nov 96, subject: Year 2000 Fixes Top Priority, November 1996
42. Rome Laboratory, Common User Baseline for the Intelligence Community (CUBIC) Configuration Management Plan, Version 1.0, 25 July 1997 (DRAFT)
43. Secretary of the Army memorandum, subject: Year 2000 Fixes Top Priority, March 1997
44. USD (Comptroller) and ASD (C3I) memorandum, subject: System Interfaces, Data Exchanges, and Defense Integration Support Tools, November 1996
45. Joint Integration Test Facility (JITF), Distributed Test Network (DTN) Concept of Operations , January 1998

APPENDIX B

DEFINITION OF TERMS

The following definitions are not intended to provide a comprehensive discussion of the terms but rather a brief synopsis related to their use within this specification.

- ***Accreditation*** – Accreditation is the formal declaration by an accrediting authority that IMA or network is approved to operate. Details on security guidance for migration systems can be found in the *DoDIIS Developer's Guide for Automated Information Systems (AIS) Security in DoD Intelligence Information Systems.*

- ***Client process*** – Client processes make requests for service from server processes (see below). After making a request, the client process waits for the response that contains the results of the request. Client processes typically are application programs that are executed by users, but system processes may also be client processes.

- **CUBIC** - A standard set of CM processes used to facilitate communication, to log, track and monitor critical information between users, PMOs and the Test Agencies.

- ***DoDIIS Configuration Definition*** – A collection of segments from DII COE and selected mission applications from a community. The DoDIIS configuration definition eases installation and configuration and provides a set of functionalities (e.g., web server, intelligence mission application server, data base server, and intelligence client). Sites may install predefined configuration definitions or can customize the installation to suit site-specific requirements.

- ***Independent Verification and Validation (IV&V)*** – IV&V is the process of evaluating a software product, such as an IMA, to determine if all functional requirements allocated to that product have been adequately implemented, that the IMA does what it is designed to do, and that the IMA meets the requirements of its users. *(The totality of the IV&V as applied to IMAs is TBR).*

- ***Integration*** – Integration is the process by which applications and data processing systems are incorporated into the computing environment. Integration can be as simple as loading the application onto the workstation and executing it. Levels of integration range from stand-alone (peaceful coexistence) to a shared environment (databases and executable components). Integration also refers to combining segments to create a system. (See Segment Integration)

- ***Intelligence Mission Application (IMA)*** – An IMA is a software module or set of software modules designed for a specific task. IMAs are distinguished from operating system software in that IMAs typically are executed by users to perform mission or task related functions such as message handling, word processing, or data analysis; while operating system software primarily manages the resources of the computer platform. IMAs may be self-contained and not require data or other resources from other processes or may be designed to execute as client processes. IMAs may consist of both client processes and server processes.

- ***Interoperability*** – Interoperability refers to the ability of two intelligence mission applications or intelligence segments to exchange data with no loss of precision or other attributes, in an unambiguous manner, in a format understood by both applications, and the interpretation of the data is precisely the same.

- ***Segment Integration*** – Segment Integration refers to the process of ensuring segments work correctly within the COE runtime environment; that they do not adversely affect one another; that they conform to the standards and specifications described in this document; that they have been validated by the COE tools; and that they can be installed on top of the COE by the COE installation tools.

- ***Server*** – Workstations (see below) offer a wide range of computing power from small machines best used by a single person to powerful systems that can support several users simultaneously. A workstation can run client processes, server processes, or a combination of client and server processes. A workstation that is dedicated to executing server processes is termed a *server*.

- ***Server process*** – Server processes listen for requests for service from client processes. The client-server concept is useful in a broad range of functions from centralized file and data storage to distributed, synchronized timekeeping.

- ***System*** – In the context of this document, a system is an amalgamation of mission applications, computing infrastructure, and commonly used support software that appears to the user as a unified whole. Software systems typically incorporate common strategies for software installation, integration, management, data interoperability, and architecture to achieve this unity. Such systems are described by documentation that specifies the architecture, integration conventions, and overall system management.

- ***Workstation*** – In the most general sense, the workstation is the hardware platform (processor, display, keyboard, etc.) and software (operating system plus other tools) that executes programs.

- ***Virtual Test Folder (VTF)*** – A website maintained by the JITF and containing all test process information to facilitate the Command feedback portion of the DoDIIS migration systems certification process. The VTF allows quick and timely access to test process information including, but not limited to, the Joint Test Planning Meeting

(JTPM) memorandums; test plans; work plans; test reports from the JITF, the JITC, and the DIA and Service security certifiers; DIA training certificates; and BETA II test results.

APPENDIX C

ACRONYMS AND ABBREVIATIONS

This listing covers the main text and the Appendices.

ABI	Application Binary Interface
AI	Action Item
AIS	Automated Information System
API	Application Program Interface
COE	Common Operating Environment
CONOPS	Concept of Operations
COTS	Commercial off the Shelf
CR	Change Request
CRR	Certification Readiness Review
CSE-SS	Client Server Environment - System Services
CUBIC	Common User Baseline for the Intelligence Community
DAA	Designated Approving Authority
DExA	DoDIIS Executive Agent
DIA/DR	Director of the Defense Intelligence Agency
DII	DoD Information Infrastructure
DII-COE	DoD Information Infrastructure – Common Operating Environment
DMB	Defense Management Board
DoDIIS	Department of Defense Intelligence Information System
DRR	Document Review Report
DT&E	Developmental Test and Evaluation
DTN	Distributed Test Network
ERB	Engineering Review Board
GOTS	Government off the Shelf
GUI	Graphical User Interface
HP	Hewlett-Packard
I&RTS	Integration and Runtime Specification
IA	Information Assurance
IAW	In Accordance With
ICD	Interface Control Document
IIPF	Intelligence Information Processing Facility
IMA	Intelligence Mission Application
INFOSEC	Information Security
IPAT	In-plant Acceptance Testing
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
ITMRA	Information Technology Management Reform Act (of 1996)

JITC	Joint Interoperability Test Command
JITF	Joint Integration Test Facility
JTA	Joint Technical Architecture
JTPM	Joint Test Planning Meeting
JTRR	Joint Test Readiness Review
JWICS	Joint Worldwide Intelligence Communications System
LAN	Local Area Network
MFR	Memorandum for Record
MS/DOS	Microsoft – Disk Operating System
MSS	Management Support System
NFS	Network File System
NIMA	National Imagery and Mapping Agency
NIS	Network Information Service
NLT	No Later Than
NT	New Technology
OS	Operating System
PMO	Program Management Office
POC	Point of Contact
PM	Program Manager
PMO	Program Management Office
PR	Problem Report
RDD	Requirements Definitions Document
SA	System Administrator
SASS	(DoDIIS) System Acquisition and Services Support
SAT	Site Acceptance Test
SECONOPS	Security Concept of Operations
SGI	Silicon Graphics
SIMO	System Integration Management Office
SIPRNET	Secret Internet Protocol Routing NETwork
SRS	Software Requirements Specification
SY2KABI	Sun Year 2000 Application Binary Interface
T&E	Test and Evaluation
TCP/IP	Transmission Control Protocol/Internet Protocol
TEM	Technical Exchange Meeting
TPOC	Test Process Oversight Committee
TS/SCI	Top Secret/Sensitive Compartmented Information
U&S	Unified and Specified
VDD	Version Description Document
VTC	Video Teleconference
VTF	Virtual Test Folder
Y2K	Year 2000

APPENDIX D

JOINT TEST PLANNING MEETING (JTPM)

Planning Questionnaire
&
Data Gathering Form

1. JTPM for ***System:*** Name: _____ Version: _____

2. Is this system applying initial certification or has a previous version been tested?

3. Today's date is : _____

4. Who is the ***System DExA***? _____Phone: _____

   a. Was the ***System DExA*** notified? _____ if so, Date: _____

5. Who is the ***PM***? _____Phone: _____

   a. Was the ***PM*** Notified? _____if so, Date: _____

6. Who is the System Developer? _____Phone: _____

   a. Was the System Developer Office Notified? _____ if so, Date: _____

7. What Agency/Service has IA/INFOSEC responsibility: **__ DIA __USAF __USA __USN**

   a. Who was notified? Name:_____Phone: _____

8. Is the release classified as: **__Major __ Minor __ Maintenance**

9. ***Scope of change***

   a. List any Certification Process **PRs/CRs** fixed from the previous version. If fixes were not made, supply the estimated timeline for the fix?

   b. List any Operating System (OS) Version Upgrades (e.g., Solaris 2.5.1 to Solaris 2.6).

c. List any OS Platform Changes (e.g., supporting Solaris and adding NT as supported OS).

d. List any Hardware Platform Changes (no change in OS, e.g., Sun SPARC to Sun Ultra).

e. List any Functionality Changes.

f. List any additional System Interfaces.

g. List any additional Integration Requirements.

h. List any New Standards that are applicable to the system (e.g., Message and NITF).

i. Does the upgrade address Year 2000 fixes?

j. What is the system Infrastructure? **___CSE-SS ___DII-COE**

10. ***IPAT testing***:

a. Date: _____ Location: _____

b. IPAT POC: Name: _____ Phone: _____

11. ***JITF testing***:

a. What is the JITF test schedule? Dates (inclusive): _____

b. JITF POC: Name: _____ Phone:_____

12. ***JITC testing***:

a. What is the JITC test schedule? Dates (inclusive): _____

b. JITC POC: Name: _____Phone:_____

13. ***Security Certification (INFOSEC):***

a. What is the INFOSEC test schedule? Dates (inclusive): _____

b. INFOSEC POC: Name: _____ Phone:_____

14. ***Training Certification:***

    a. What is the Certification schedule? Dates (inclusive):_____

    b. Certifier POC: Name: _____ Phone:_____

15. ***BETA II testing:***

    a. What is the BETA II Test schedule? Dates (inclusive): _____

    b. BETA Site POC: Name: _____ Phone:_____

    c. BETA II Site location: _____

    d. BETA II Site selection criteria: _____

16. List any ***optional testing***.

APPENDIX E

JTPM MEMO FOR RECORD

1. SYSTEM:

2. PURPOSE:

3. DATE OF JTPM and LOCATION:

4. PARTICIPANTS:

a. *DExA for T&E Rep:*
b. *(System) DExA Rep:*
c. *(System) Program Manager Rep:*
d. *(System) Developer Rep:*
e. *JITF Rep:*
f. *JITC Rep:*
g. *Security Certifier:*
h. *Training Certifier:*
i. *BETA II Site Rep:*

5. CERTIFICATION SUMMARY: (reference JTPM Planning Questionnaire [Appendix D])

a. *Type of Release (Major, Minor, Maintenance)*
b. *Scope of Change*
c. *IPAT Testing (test dates, POCs, etc.)*
d. *JTRR (date, documentation-determination to proceed, POCs, etc.)*
e. *JITF Testing (scope of testing, test dates, POCs, etc.)*
f. *JITC Testing (scope of testing, test dates, list of interfaces, test plan publication date, POCs, etc.)*
g. *Security Testing (scope of testing, test dates, test site, POCs, etc.)*
h. *Training Certification (where conducted, by whom, to whom)*
i. *BETA II Testing (scope of testing, test dates, test site, POCs, etc.)*

6. GENERAL COMMENTS:

7. **OUTSTANDING ISSUES:** *(Between whom, nature of issue, where to be resolved)*

8. POC FOR THIS MEMO:

Attachment:
DoDIIS Migration System Certification/Re-Certification Assessment Matrix

DoDIIS Migration System Certification/Re-Certification Assessment Matrix

SYSTEM

TEST EVENTS	IPAT	Install	Integrate	DII/COE Comply	CSE Comply	Interop	Security	BETA II	Training
Type of Change									
Platform Change									
Operating System (OS) Version Upgrade (e.g. Solaris 2.4 to Solaris 2.5)									
OS Platform (e.g., Supporting Solaris and adding Digital UNIX as supported OS)									
Hardware Platform (no change in OS, e.g., Sun SPARC to Sun Ultra)									
Operational Impact									
Installation Procedures									
Operational Procedures									
Functionality									
Major Change in Functionality									
Minor Change in Functionality									
Maintenance Release									
Interface(s) (e.g., Interface with new system(s))									
Integration									
New Standards (e.g., Message & NITF)									
Year 2000									

APPENDIX F

JTRR MANDATORY AGENDA ITEMS

1. Agenda. The following form the basis for the JTRR Agenda but are not all inclusive of agenda items that may be discussed:

a. Verification that all required documentation has been provided. If not, the scheduled test will be cancelled until documentation can be produced. The DExA for T&E shall coordinate with the JITF to establish a new test date.

b. Workplan Review and JITC Test Plan Review.

c. Verification that all required hardware and software are available.

d. PMO certification of successful DT&E completion/discussion of IPAT findings.

e. Discussion of any open Change Requests (CRs), Problem Reports (PRs), and Document Review Reports (DRRs) that may exist against the baseline system.

f. Identification of the level of anticipated user participation.

g. Verification that appropriate personnel clearances have been provided to the Air Force Research Laboratory Security Office.

h. Review system documentation updates and the availability of documents for JITF/JITC/Security testing.

i. Finalize the detailed schedule of test activities.

j. Resolution of any outstanding issues.

APPENDIX G

BETA II TESTING RECOMMENDATIONS

SECTION G.1

BETA II SITE SELECTION

The PMO is responsible for selecting a BETA II site early in the development cycle to allow for adequate preparation and coordination for this phase of testing. More than one BETA II site may be selected to ensure complete testing of all required operational platforms. All operating system platforms will require separate certifications. Typically, the BETA II site is selected before the first System Design Review (SDR) or during the System Readiness Review (SRR) meeting.

a. The PMO will choose BETA II site(s) that best represent the operation of the system within the user community and notify the JITF of their selection when they schedule the JTPM. Specific site selection considerations include:

   (1) Volunteer.

   (2) CSE-SS/DII-COE Compliant Environment.

   (3) Prime User of System Undergoing BETA II Testing.

   (4) Maximum Number of Interfacing Systems on Site.

   (5) Maximum Number of Supported Platforms.

   (6) Participant in System Development Process.

   (7) Availability of Facilities and Personnel.

   (8) Active in Review and Update of Test Plans and Procedures.

b. JITC interoperability testers will participate in BETA II site tests. JITF and/or Security Accreditors may also be present for observation and/or participation in BETA II testing. In addition, operational personnel from the BETA II site are strongly encouraged to participate in the different phases of certification testing to provide insights and to facilitate accurate testing. Section G.3.2 provides a checklist of BETA II site recommended responsibilities, and Section G.2.0 provides a checklist for required resources.

SECTION G.2.0

BETA II SITE RECOMMENDED RESOURCE CHECKLIST

G.2.1 Personnel

a. System Administrator.

b. Network Support.

c. Security (ISSO) support for accreditation and general site accesses.

d. Qualified users for functional testing as required (i.e., Site Acceptance Test).

e. Integration/Interoperability system users for end-to-end testing (same system personnel and functional users from development through testing phases).

f. Training Support On-Site trainers should be available. Most systems use a train-the-trainer approach.

g. Training of test participants to be accomplished prior to BETA II test.

h. Management Support.

G.2.2 Hardware/Software

a. Sufficient interfaces, internal and to other systems, as stated in test plans.

b. Sufficient communications (i.e., external networks) as required in test plans.

c. Up-to-date licenses (i.e., software, operating system), as required.

d. Sufficient test data (i.e., loaded databases, volume/type of message traffic) to support a large intelligence site capability.

e. Root access availability will be provided by the System Administrator, or the task requiring root access will be performed by the System Administrator.

f. If possible, testing should be kept in operational context and not moved to a separate test suite or LAN.

G.2.3 Actual Time to Conduct Test

a. Ensure major site infrastructure is stable for the duration of the test (no new systems/equipment installs scheduled).

b. Allow for resource flexibility as issues are encountered (i.e., testing may be delayed for days due to unforeseen problem).

c. Ensure no major exercise or competing event is scheduled during time of test (i.e., theater contingency support).

G.2.4 General Support

a. Make available a secure and a non-secure phone in the computer room or test area that will not interfere with day-to-day mission.

b. Provide pertinent site configuration documentation (i.e., application, O/S, and database).

c. Provide security documentation to include MIL-STDs, DIA documentation, and SCIF documentation.

d. Provide a dedicated training environment to include workstations and connections in case training is required for new users participating in BETA test.

e. Provide a copier and facsimile capability.

f. Provide a desk with PC for test team administration (If possible, a network account or other method for e-mail access for test team).

g. If possible, test team should be able to work in the same test space for the duration of the event.

SECTION G.3.0

BETA II TESTING

Upon DMB approval (see DIA Regulation 65-13), the PMO proceeds to install the system at a BETA II user site(s). The BETA II site(s) selected is chosen early in the development cycle to allow for adequate preparation and coordination for this phase of testing. The PMO validates the system functionality and stability in an operational environment during BETA II testing. BETA II testing is conducted to assess a system's operational effectiveness, user efficiency, suitability, and impact on security architecture and to identify needed modifications. The Test Agencies may also complete assessments of system performance at BETA II testing. The PMO will not make any changes to the baseline tested at the JITF except for corrections to Category I findings or due to PMO's CCB action.

G.3.1 Generation and Distribution of Findings. At the completion of BETA II, the user site provides a summary of results to the DMB for consideration. The BETA II test report format is in Section 4.0 of this Appendix.

a. A copy of this report will be sent to the DExA for T&E, Test Agencies, DoDIIS SIMO and ERB. The PMO also submits an updated ADM to the DMB/LCM requesting approval to deploy. An updated ADM should include all previous items plus the final security certification, the BETA II Test Report, and an updated status briefing.

b. In the event a change occurs to the application baseline after BETA II testing, a BETA II representative will participate in any PMO testing to validate implementation of BETA II findings.

G.3.2 BETA II Site Recommended Responsibilities. BETA II sites are responsible for:

a. Participating in the Certification Process (JTPM, Test Planning and Reports, and feedback through the VTF).

b. Sending representatives from the site System Administrator/System Support section and functional users to JTPM, IPAT, JITF, JITC, and Security Tests. (These representatives should be those who will be participating in the subsequent BETA II test.)

c. Posting the BETA II Test Report, according to the format in Section 4.0 of this Appendix, to the Command/Command SIMO Homepage that will be linked to the VTF.

d. Acquiring system documentation and JITF/JITC/Security test reports for review to support or refine development of BETA II test plans and procedures.

e. Assigning at least one System Administrator and one functional user to support and participate in BETA II testing and in any post-BETA II testing to validate implementation of BETA II findings.

f. Coordinating with and supporting the JITC for interoperability testing at the BETA II site.

g. Obtaining site authorization, coordinating requirements, and ensuring resource scheduling.

h. Completing the security site accreditation package prior to testing, i.e., written site ISSM approval to add system to site.

SECTION G.4.0

BETA II TEST REPORT FORMAT

Upon the completion of BETA II testing, a summary of the test results shall be prepared in the following format:

Program Name VERSION *x.x* BETA II TEST REPORT
[This report will summarize BETA II test results as well as clarify any unique findings at the test site. The report will be written by the BETA II site personnel with inputs from the PMO, Security and the Joint Interoperability Test Command (JITC), if applicable. This report will be prepared in message format.]

1. INTRODUCTION.

1.1 BACKGROUND. THE *site name* HAS BEEN DIRECTED BY THE DEPARTMENT OF DEFENSE INTELLIGENCE INFORMATION SYSTEM (DoDIIS) MANAGEMENT BOARD (DMB) TO CONDUCT BETA II TESTING FOR *Program Name* VERSION x.x. THIS LEVEL OF TESTING IDENTIFIES CONFLICTS AND OPERATIONAL IMPACTS OF APPLICATIONS RESIDING IN COMMON DoDIIS ENVIRONMENTS. TESTING WAS CONDUCTED BY BETA II SITE PERSONNEL WITH SUPPORT FROM SECURITY AND JITC, WHEN APPLICABLE.

1.2 PURPOSE. THE PURPOSE OF THIS MESSAGE IS TO REPORT THE RESULTS OF BETA II TESTING CONDUCTED FOR THE *Program Name* VERSION x.x PROGRAM MANAGEMENT OFFICE (PMO).
[This section will also include a purpose statement for the specific program being tested.]

1.3 OBJECTIVES. THE OVERALL OBJECTIVE OF THE BETA II TEST IS TO PROVIDE ANALYSIS AND RECOMMENDATION TO THE DMB REGARDING THE RESULTS OF THE BETA II TEST WITH A RECOMMENDATION ON WHETHER *Program Name* VERSION x.x IS READY FOR PRODUCTION AND DEPLOYMENT. THE SPECIFIC OBJECTIVES OF THE BETA II TESTING PROCESS FOR *Program Name* VERSION x.x ARE: INSTALLATION USING THE CONFIGURATION AND INSTALLATION GUIDE PROVIDED BY THE PMO, SUPPORT SECURITY TESTING, SUPPORT INTERFACE TESTING IN COORDINATION WITH THE JITC, AND ...*[add any other program specific objectives]*.

1.4 RECOMMENDATION. BASED UPON THE FOLLOWING RESULTS, *site name* RECOMMENDS/DOES NOT RECOMMEND PRODUCTION AND DEPLOYMENT OF *Program Name* VERSION x.x AS A SUCCESSFULLY/UNSUCCESSFULLY

INSTALLED, FUNCTIONALLY TESTED, AND ACCREDITED/NON-ACCREDITED SYSTEM. *[Or use some similar statements.]*
[This section will state the BETA II site's recommendation for fielding the specific program.]

2. TEST ENVIRONMENT.
[This section will summarize the hardware and software configuration used for testing. The configuration should identify each workstation and server used and their roles in the configuration. The server and client configuration should identify the hardware platform, operating system, and software used during the testing.]

3. TEST RESULTS.

3.1 INSTALLATION.
[The section will explain hardware and software installation results based on installation and configuration guides.]

3.2 FUNCTIONALITY.
[This section will explain the program functionality tested and the results based on test criteria from the users.]

3.3 SECURITY. SECURITY TESTING WAS PERFORMED ON dd mmm yyyy. THE SECURITY REPRESENTATIVE FROM xxxxxx WAS PRESENT FOR TESTING AND PROVIDED THE FOLLOWING INPUTS. *[Include inputs from security office.]*

3.4 INTEROPERABILITY (If applicable). INTEROPERABILITY TESTING WAS PERFORMED ON dd mmm yyyy. THE JITC REPRESENTATIVE WAS PRESENT FOR TESTING AND PROVIDED THE FOLLOWING INPUTS. *[Include inputs from JITC.]*

4. ANALYSIS.

4.1 FINDINGS PROHIBITING DEPLOYMENT.
[This section will state whether there were findings prohibiting deployment. If there are such findings, please justify.]

4.2 FINDINGS REQUIRING RESOLUTION.
[This section will state whether there were findings requiring resolution. If there are such findings, please justify.]

4.3 AREAS OF CONCERN.
[This section will describe any areas of concern.]

5. PARTICIPANTS.
[This section will list the name, test responsibility, organization, and telephone number of each BETA II test participant.]

APPENDIX - PRs, CRs, DRRs.

[This appendix will list all Problem Reports, Change Requests, and Document Review Reports generated during the BETA II test, with comments.]

APPENDIX H

BETA I AND BETA II PMO SECURITY CERTIFICATION LETTER FOR INTELLIGENCE MISSION APPLICATIONS (IMAs)

MEMORANDUM FOR: Program Management Office/System
Attn: Organization/Division (Person)
Mailing Address

FROM: Certifying Authority

SUBJECT: BETA I or BETA II Security Certification for the (System Tested), Version (Version Number)

Reference: a. DIA Manual 50-4, 30 April 1997, "Department of Defense (DoD) Intelligence Information System (DoDIIS) Information Systems Security (INFOSEC) Program."

b. DCID 1/16, 19 July 1988, "Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks."

c. DoDIIS Developer's Guide for Automated Information Systems (AIS) Security in Intelligence Information Systems, November 1993.

d. Joint DoDIIS/Cryptologic SCI Information Systems Security Standards, 1 March 1998

e. DCID 6/3. Date TBD, “Security Intelligence Information Systems Processing National Intelligence Information” (Draft)

1. The ***(System Name)*** IMA Version ***(Version Number)*** BETA **(I *or* II)** security certification test was executed under the direction of ***(Certifying Authority)*** at (**the Joint Integration Test Facility (JITF), Rome N.Y.,** or ***Site Location***) on ***(Date)***. The results of the tests demonstrated conformance to minimum computer security requirements as defined in

references a. through e. for processing Top Secret, Sensitive Compartmented Information (SCI) in a System High Mode of Operation. ***(Enter Discrepancies if any.)*** No major discrepancies were noted during the test. Minor discrepancies are provided in the enclosure.

2. Based on the favorable results of the BETA **(I** or **II)** security test, ***(Certifying Authority)*** recommends that the DoDIIS Management Board (DMB) approve ***(System Name)*** IMA Version ***(Version Number)*** to be deployed **(to BETA II sites for installation and certification testing**, or **operationally).**

3. The Information Assurance or INFOSEC Action Officer is ***[Action Officer name]***. This Action Officer can be reached at DSN ***[xxx-xxxx]***, or Commercial ***[(xxx) xxx-xxxx]***.

Signature Block

cc:
DMB/ERB/SIMO
DIA/SYS-4
497IG/IND (DExA for T&E)

Encl:
(System Name, BETA I or II) Test Results

APPENDIX I

DoDIIS IMA VERSION RELEASE POLICY

The DoDIIS IMA Certification Process, as defined in the Instructions to the DExAs, PMOs and Developers, outlines the procedures for receiving DMB approval to field a software release to a DoDIIS site. PMOs will classify and number their software applications according to the guidance below. Any dispute about the categorization of a release and the type of required testing will be raised to the DMB by the DExA.

I.1.0 ***Version Release Classification.*** The following policy, defined by the DMB, applies to initial and follow-on releases of a system. Releases of DoDIIS IMAs are to be categorized as major, minor, or maintenance as defined in the *DII COE Integration and Runtime Specification (I&RTS), Version 3.0.* Releases of segmented IMAs include:

- Major releases identified as 'n.0' "indicates a significant change in the architecture or operation of the segment. Compatibility libraries will be provided if necessary to preserve backward compatibility."
- Minor release identified as 'n.n' "in which new features are added to the segment, but fundamental segment architecture remains unchanged. A minor release may necessitate re-linking to take advantage of updated API libraries, but APIs are preserved at the source code level except possibly on a documented basis with the explicit approval of the DISA CCB."
- Maintenance releases - identified as 'n.n.n' "in which new features may be added to the segment, but the emphasis is on optimization, feature enhancements, or modifications to improve stability and usability. APIs are preserved and do not generally require segments to recompile or re-link during successive releases."

I.2.0 ***Software Version Numbering.*** In addition, the PMO is responsible for assigning the system version release number in accordance with the DoDIIS numbering system as show above. This numbering system is a variant of the DII COE numbering system and will ensure a consistent numbering convention throughout the community. DoDIIS version numbers consist of a sequence of three-integer placeholders, separated by decimal points, in the following format:

a.b.c

Each of the three digits has a specific meaning. The first digit indicates a *major release* number; the second digit indicates a *minor release*; and the third digit indicates a *maintenance release* number. For example,

1.0 - Initial Major Release for System A

1.1 - Initial Minor Release for System A

1.1.1 - Initial Maintenance Release for System A

APPENDIX J

TRAINING CERTIFICATION

J.1.0 Training Certification. Training Certification is conducted to ensure systems have an adequate training plan and have planned for the required resources to implement that plan. DoDIIS IMA PMOs will request training certification 30-45 days prior to ADM presentation to the DMB. This request should include the current training plan (which may be included in the training section of an installation logistics support plan) and Program of Instruction (POI). Detailed lesson plans/manuscripts may be represented by course control documentation providing lesson learning objectives. Other information which demonstrates PMO training to support testing or fielding will be included.

Forward request and information to: ***Chairman***
General Intelligence Training Council
ATTN: DAJ-GI
Washington, DC 20340-5100

It is recommended that PMOs call or contact the GITS division to coordinate this action, since each IMA is at different levels of system life cycle.

a. Pending development of a training certification checklist, the following guidelines/criteria are provided:

(1) Is the training plan (TMP/ILSP) current and does it include pertinent training/training resource data?

(2) Has pilot training been conducted and with what results?

(3) Is (are) the training target population(s) identified in terms of numbers and locations?

(4) Does the Program of Instruction/lesson materials identify the learning objectives based upon the system's critical tasks?

b. In addition to the above criteria, the following items will be examined:

(1) Are surge (installation) training and sustainment (steady state) training adequately covered?

(2) Has coordination been made with users and service intelligence schools?

(3) Are training resources adequate for near term and out years?

(4) Has a responsible training authority been identified to maintain the system training and has consideration been provided to integrate such training into functional intelligence course(s)?

Results of Training Certification will be posted on INTELINK and the VTF.

APPENDIX K

JITF – PASS/FAIL CRITERIA FOR INTEGRATION TESTING

Reporting Codes

The following codes are used by JITF test teams to indicate the severity of impact or significance of each integration finding.

Impact 1

A finding that, without resolution, either

a) prevents the IMA from proceeding further in testing or operation;
b) prevents either the IMA or another application or component of the infrastructure from operating properly;
c) creates a security vulnerability in the IMA or site architecture that can be exploited by a general user without taking advantage of other vulnerabilities or capabilities; or
d) seriously increases the level of effort of site personnel to manage and/or use the IMA or other applications.

No workaround is available during the testing period, and the resolution requires a significant level of effort on the part of the IMA developer and (possibly) other agents to implement, validate, and incorporate into the IMA baseline.

Impact 2

A finding that, without resolution,

a) prevents the IMA from proceeding further in its testing or operation;
b) has a significant effect on the operation of either the IMA or on another application or component of the infrastructure; or
c) creates a security vulnerability in the IMA or site architecture that could be exploited by a general user only if the user is able to take advantage of other vulnerabilities or capabilities not typically available to him or her.

The finding can be temporarily resolved by a workaround that is implemented as a change in procedure or configuration. The successful implementation of the workaround requires technical expertise that is not expected of general users, or the workaround requires a significant level of effort by site administrators. The workaround does not cause significant delay in integration testing; instead, it can be proposed and evaluated during integration testing at the JITF.

Impact level 2 findings may cause integration test failures depending upon the level of effort required to implement a workaround (and confidence in it). An Impact 2 problem

may be elevated to an Impact 1 if proposed workarounds either do not work successfully or produce additional Impact 2 and 3 findings.

Impact 3

A finding, that without resolution has a significant effect on the operation of either the IMA or on another application or component of the infrastructure. The finding can be temporarily resolved by a workaround that is implemented as a change in procedure or configuration. The successful implementation of the workaround does not require technical expertise that is not expected of general users, or the workaround does not require a significant level of effort by site administrators. The workaround does not cause significant delay in integration testing; instead, it can be proposed and evaluated during integration testing at the JITF.

Impact 3 findings generally do not cause integration test failure unless the number of findings increases the level of concern about the overall quality of the IMA.

Impact 4

A finding that does not prevent the IMA from proceeding further in its testing or does not significantly affect the operation of the IMA or another application or component of the infrastructure. The finding can be resolved by a workaround that can be implemented as a change in procedure or configuration during integration testing without a significant level of effort, or the finding can be left as is. Even though the finding has some affect on the configuration or operation of the IMA or of other components of the site architecture, the general user will be able to perform mission functions, and the administrator will be able to manage the IMA. Findings in this category are of lesser importance, but the accumulation of Impact 4 findings may result in an overall finding at a higher Impact level.

APPENDIX L

JITC – RECOMMENDATION TO PROCEED CRITERIA

L1. Recommend Proceed. Recommend proceed indicates the IMA meets ALL or SOME of the joint interoperability requirements defined by the users, and the unmet requirements resulted in only MINOR operational impacts. Based upon the interfaces available for test during Beta I, the JITC recommends the IMA proceed to the next step in the certification process.

L2. Recommend Conditional Proceed. Recommend conditional proceed indicates the IMA meets SOME of the joint interoperability requirements defined by the users, and the unmet requirements resulted in MAJOR operational impacts. Based upon the interfaces available for test during Beta I, the JITC recommends that the IMA proceed to the next step in the certification process only if the unmet requirements are scheduled for prompt resolution within six months.

L3. Recommend Do Not Proceed. Recommend do not proceed indicates the IMA does not meet joint interoperability requirements defined by the users, or only meets SOME of the joint interoperability requirements, and the unmet requirements resulted in SIGNIFICANT operational impacts. Based upon the interfaces available for test during Beta I, the JITC recommends the IMA not proceed to Beta II until the unmet requirements are resolved.

APPENDIX M

DOD YEAR 2000 COMPLIANCE CHECKLIST

Note: The following check list (Appendix M) is a verbatim copy of the check list found in the *DoD Year 2000 Management Plan*, Version 1.0, April 1997, Appendix B.

The purpose of this checklist is to aid system managers in ensuring their systems are compliant for the Year 2000. Make sure the following items are included in your Year 2000 testing and compliance process for all of the developed, gratis, licensed, and purchased software, hardware, and firmware used in your system's operation, development/maintenance, support, and testing activities.

Y2K compliant system accurately processes date/time date from, into and between the twentieth and twenty-first centuries and the leap year calculations. Finally, "compliant" systems have no extended semantics, calendar errors, date overflow, and inconsistent semantics.

Please respond to each question with the appropriate answer.

System Identification

(An asterisk indicates an optional question)

1. Please provide system information.

   a. Name of system _____

   b. Defense Integration Support Tools (DIST) Number of system _____

   c. Operational date of system (current or a future date)* _____

   d. Planned or actual replacement date of system (retirement or discontinuation qualifies as replacement)* _____

e. For planned replacements what is the contingency plan and under what conditions will it be invoked?* _____

f. What are the safety critical portions of the system, if any?* _____

Year 2000

2. Each system has its own window of time, before and after the present date, in which it functions. Planning and scheduling systems work with dates that are weeks, months, and sometimes years in the future. Likewise, trend analysis systems and billing systems regularly reference dates in the past. For your system, and its window of time, please verify its ability to successfully process data containing dates with no adverse effect on the application's functionality and with no impact on the customer or end user beyond adjustment to approved changes in procedures and data formats.

		VERIFIED	NO	N/A
a.	Dates in 20th century (1900s)			
b.	Dates in 21st century (2000s)			
c.	Dates across century boundary (mix 1900s and 2000s)			
d.	Crosses 1999 to 2000 successfully			

Other/Indirect Date Usage

3. Have you verified performance (and corrected if necessary):

		VERIFIED	NO	N/A
a.	Dates embedded as parts of other fields			
b.	Dates used as part of a sort key			
c.	Usage of values in date fields for special purposes that are not dates (e.g. using 9999 or 99 to mean "never expire")			
d.	Date dependent activation/deactivation of passwords, accounts, commercial licenses, etc.			
e.	Date representation in the operating system's file system (creation dates and modification dates of files and directories)			
f.	Date dependent audit information			
g.	Date dependencies in encryption/decryption algorithms			
h.	Date dependent random number generators			
i.	Date dependencies in firmware			
j.	Personal Computer BIOS and RTC does not reset the year to 1980 or 1984 on reboots after 31 December 1999*(Corrections by operating system utilities are allowed.)*			

Leap Year

4. System accurately recognizes and processes Year 2000 as a leap year.

	VERIFIED	NO	N/A
a. February 29, 2000 is recognized as a valid date			
b. Julian date 00060 is recognized as February 29, 2000			
c. Julian date 00366 is recognized as December 31, 2000			
d. Arithmetic operations recognize Year 2000 has 366 days			

Usage of Dates Internally

5. Internal application usage of dates and date fields must be clear and unambiguous in the context of the systems which use them.

	VERIFIED	NO	N/A
a. Display of dates is clear and unambiguous (the ability to correctly determine to which century a date belongs either by explicit display, i.e. 4-digit year, or system or user inference)			
b. Printing of dates is clear and unambiguous			
c. Input of dates is clear and unambiguous			
d. Input of logically correct dates			
e. Storage of dates is clear and unambiguous			

External System Interfaces

6. External interactions are identified and validated to correctly function for all dates.

	VERIFIED	NO	N/A
a. Interaction between this system and any other external time source, if existing, has been verified for correct operation.			
For example, the GPS system is sometimes used as a time source. Many GPS receivers cannot correctly deal with theroll-over of the GPS 10-bit epoch counter that will occur at midnight, 21 August 1999. GPS receivers also deal with an 8-bit Almanac Week counter which has a 256-week roll-over span.			
b. You and the responsible organization for each interface have negotiated an agreement dealing with Year 2000 issues.			
For example, is the interface currently Y2K compliant, is it being worked on, does it have an unknown fix date, or will it be fixed by a future date you have mutually agreed on.			

For each interface that exchanges date data, you and the responsible organizations have discussed and verified that you have implemented consistent Year 2000 corrections that will correctly work for date data passed between your systems.

Date Field Type

7. Describe the type of date fields used by the system, in either software ordata bases.

	VERIFIED	NO	N/A
a. Does the system use 4-digit year data fields?			
b. Does the system use 2-digit year data fields?			
c. If 2-digit, does the system use a century logic technique to correctly infer the century?			
d. At what date will the century logic fix fail?			

	YES	NO
e. Are there any internal data types for dates?		

If yes to e, what is the range of dates that the date field can represent?

Minimum Date _____ Maximum Date _____

Year 2000 Testing Information

8. Optional: Please provide the following information with regard to testing the application for Year 2000 compliance:

	Narrative Answer
a. Testing Organization	
b. Name of Test Team Chief	
c. Date that Year 2000 compliance testing was completed	
d. How was Year 2000 compliance determined? (certified by vendor or contractor, tested in-house, inspected but not tested, etc.)	

	YES	NO
e. Are the test data sets available for regression testing on the next version release for questions 2, 3, 4, 5, 6, 7d, and 7e?		
f. Are the detailed test results and reports available for reviewand audit for questions 2, 3, 4, 5, 6, 7d, and 7e?		
g. Do you follow a defined process for tracking the status of all Year 2000 problems reported, changes made, testing, compliance, and return to production?		

COTS/GOTS Components

9. Optional: Please provide the following information with regard to COTS/GOTS components.

		YES	NO	N/A
a.	Does the system use COTS/GOTS application packages and/or infrastructure components?			
b.	If yes, have those items been verified to be Year 2000 compliant?			

Narrative Answer

c. How was Year 2000 compliance determined? (certified by vendor or contractor, tested in-house, etc.) _____

Certification Levels

Certification levels are defined below. Yes, verified and N/A are considered positive responses. No is considered a negative response.

LEVEL

0 System retired or replaced

1 Full independent testing completed with either:

- All questions have positive responses except possibly 7b or
- All questions have positive responses except possibly 7a

2 Independent audit of system and existing testing completed with either:

- All questions have positive responses except possibly 7b or
- All questions have positive responses except possibly 7a

3 Self-certification

CAUTION: Self-certification assumes a higher risk level of potential failures

3a Self-certification with full use of 4-digit century date fields

- All questions have positive responses except possibly 7b

3b Self-certification indicates risk due to use of 2-digit century fields

- All questions have positive responses except possibly 7a

3c Self-certification indicates risk due to ambiguous usage of dates

- Question 5-a,b,c or d have negative responses.

3d Self-certification indicates potential problems (System needs additional work before Year 2000 processing can be assured with any level of reliability)

- Question 2-a,b,c or d have negative responses, or
- Question 3-a,b,c,d,e,f,g,h,i or j have negative responses, or
- Question 4-a,b,c or d have negative responses, or
- Question 5-a,b,c or d have negative responses, or
- Question 6-a or b have negative responses, or
- Question 9-b has a negative response.

4 Not certified or not certified yet.

It would be advisable but not required for the system/program/project manager to have the responsible programmer(s) fill out a similar checklist covering the software they are responsible for before completing this checklist for the overall application.

LEVEL OF CERTIFICATION FOR THIS DATA SYSTEM: (*Circle only one)*

0 1 2 3a 3b 3c 3d 4

I certify that the information provided above is true and correct to the best of my knowledge and belief:

ADDITIONAL
COMMENTS:_____
_____
_____
_____

_____ _____

System Manager Date

I certify that the information provided above is true and correct to the best of my knowledge and belief:

ADDITIONAL
COMMENTS:_____
_____
_____
_____

_____ _____

System Customer Date