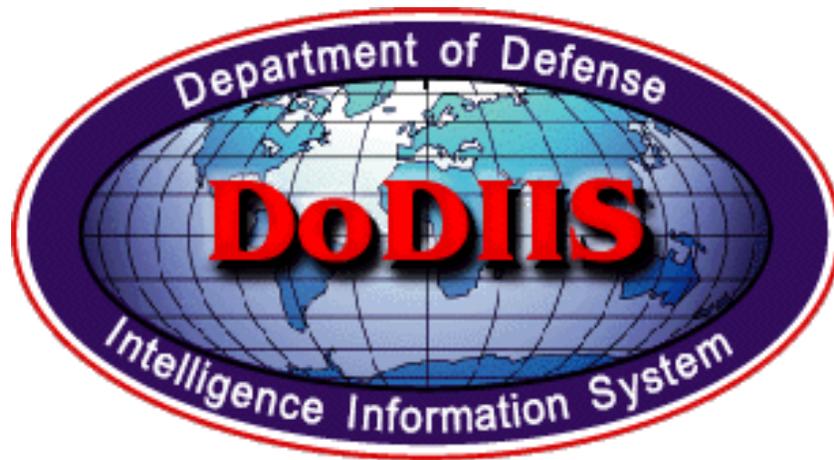


UNCLASSIFIED



**Test and Evaluation Policy
for
Department of Defense Intelligence
Information System (DoDIIS)
Intelligence Mission Applications (IMAs)**

March 2004

Prepared by:

DODIIS DExA for Test & Evaluation (T&E)
AFC2ISRC/INYE
219 Dodd Blvd Building 661
Langley AFB, Virginia 23665
email: dexa.te@langley.af.mil

UNCLASSIFIED

UNCLASSIFIED

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Approval of the Test & Evaluation Policy for Department of Defense Intelligence Information System (DoDIIS) Intelligence Mission Applications (IMAs)

1. The Test & Evaluation Policy for DoDIIS IMAs shall be effective upon review and signature of the below party. 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 DoDIIS Executive Agents (DExAs), Program Managers (PMs) and the Community of Test Agencies responsible for developing and testing IMAs 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 dexa.te@langley.af.mil

/s/ Kelly Fesel, 1st Lt, USAF
DoDIIS Executive Agent, Test and Evaluation

Date: March 2004

TABLE OF CONTENTS

MEMORANDUM FOR DISTRIBUTION..... I

TABLE OF CONTENTSII

LIST OF FIGURES..... III

EXECUTIVE SUMMARYIV

SECTION 1 – BACKGROUND AND INTRODUCTION5

 1.1 BACKGROUND5

 1.2 INTRODUCTION6

 1.3 PURPOSE.....6

 1.4 SCOPE6

SECTION 2 - TEST AND EVALUATION OBJECTIVES.....9

SECTION 3 - TESTING MILESTONES & EVENTS 10

 3.1 JOINT TEST PLANNING MEETING (JTTPM)..... 10

 3.2 IN-PLANT ACCEPTANCE TESTING (IPAT)..... 11

 3.3 SOFTWARE BASELINE 12

 3.4 DOCUMENTATION REVIEW 12

 3.5 JOINT TEST READINESS REVIEW (JTRR)..... 13

 3.6 JITF TESTING..... 14

 3.7 JITC TESTING..... 17

 3.8 INFORMATION ASSURANCE (IA) (SECURITY) TESTING 19

 3.9 TRAINING CERTIFICATION..... 21

 3.10 BETA II TESTING..... 22

SECTION 4 - DODIIS TEST & EVALUATION PROCESS DESCRIPTIONS AND RESPONSIBILITIES..... 25

 4.1 DoDIIS EXECUTIVE AGENT (DEXA) FOR TEST & EVALUATION (T&E)..... 25

 4.2 DOCUMENT AND REPORT REQUIREMENTS 25

 4.3 TEST PROCESS OVERSIGHT COMMITTEE (TPOC)..... 25

 4.4 TEST METRICS 26

 4.5 VIRTUAL TEST FOLDER (VTF)..... 26

 4.6 SECURITY VIRTUAL TEST FOLDER (SVTF)..... 26

 4.7 DISTRIBUTED TESTING NETWORK (DTN)..... 26

 4.8 TESTING CONFIGURATION MANAGEMENT (CM)..... 26

 4.9 TEST ORGANIZATIONS 27

SECTION 5 – REVIEW AND TERMINATION 30

APPENDIX A – REFERENCES..... 31

APPENDIX B - DEFINITION OF TERMS..... 33

UNCLASSIFIED

APPENDIX C - ACRONYMS AND ABBREVIATIONS.....35

**APPENDIX D – JOINT TEST PLANNING MEETING (JTPM) SCHEDULING
CHECKLIST 37**

APPENDIX E - JTPM MEMORANDUM FOR RECORD39

APPENDIX F - JTRR MANDATORY AGENDA ITEMS 43

APPENDIX G - BETA II TESTING RECOMMENDATIONS 44

 SECTION G.1 BETA II SITE RECOMMENDED RESOURCE LIST 44

 SECTION G.2 BETA II SITE CONFIRMATION LETTER MEMORANDOM..... 45

 SECTION G.3 BETA II TEST REPORT FORMAT 46

**APPENDIX H - BETA I AND BETA II PMO SECURITY CERTIFICATION LETTER
..... 48**

APPENDIX I - DODIIS IMA VERSION RELEASE POLICY..... 50

LIST OF FIGURES

Figure 1-1 DoDIIS Certification Process 7

UNCLASSIFIED

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*.
- Provides guidance to testing agencies responsible for certifying IMAs for compliance with the DoDIIS Profile.
- Provides certification process guidance to the PMs and DExAs responsible for supervision of IMA development and testing.
- Provides a series of appendices, references, checklists and guides to assist with the preparation of testing and post-test milestones to the PMs, Testers, System Administrators and Application Users.
- DoDIIS IMAs are developed individually by the Services and the Defense Intelligence Agency (DIA), funded through the General Defense Intelligence Program (GDIP), managed by the DExA for T&E, and overseen by the DoDIIS SIMO and the DMB.

Note: Dates are in calendar days except where listed as business days.

UNCLASSIFIED

SECTION 1 – BACKGROUND AND INTRODUCTION

1.1 Background. In June 1995, the Combatant 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 Defense Intelligence Agency (DIA)/DR approved the DoDIIS AIS Certification Process for all DoDIIS AISs destined for installation at DoDIIS sites. To focus attention on the Intelligence Community (IC), AIS applications shared among DoDIIS Sites were re-designated Intelligence Mission Applications in 1998. The DoDIIS Intelligence Mission Application (IMA) Certification Process is described in the *DoDIIS Instructions* document, which is scheduled for update on an annual basis.

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, responsible for IMA integration evaluation, verifies IMA compliance with the DoDIIS Infrastructure and at the request of DIA/SYS-4 performs Vulnerability Assessments (VA) on tested IMAs. 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*.
- National Geospatial-Intelligence Agency (NGA) Integration Test Facility (ITF): performs the same functions as the JITF for NGA acquired IMAs, conducts security testing, and has a resident interoperability tester on staff, in addition to providing independent functionality testing.
- Information Security (Information Assurance (IA)) Certifiers(C): designated security certification authority for DoDIIS, responsible for validating Director of Central Intelligence Directive (DCID) 6/3 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.
- 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 NGA College: designated IMA training certification authorities, responsible for ensuring IMAs have a valid Training Management Plan.
- 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. PMOs are responsible for design and preparation of Beta II tests.
- Beta II Testing Sites: designated operational deployment assessment authorities, provides facilities and personnel for certification of IMA interoperability and functionality with

UNCLASSIFIED

other IMAs or AISs in an operational environment.

1.2 Introduction. The DoDIIS community has emphasized four objectives: **interoperability, sharable resources, security and modularity of mission applications.** The four objectives are also shared across the IC, not only because of common goals for integration and interoperability, but also because IMAs 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 to the IC. The planning and implementation by DoDIIS of a flexible architecture will offer common solutions to other IC members.

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 T&E:

Test Agencies:

- **JITF** a component of the Information Handling Branch (IFEB), Information Directorate, Air Force Research Laboratory, Air Force Material Command, at Rome, New York
- **JITC** a component of the Defense Information Systems Agency(DISA), headquartered at Ft. Huachuca, Arizona and the DoDIIS JITC group at Indiana Head, Maryland
- **IA** Certifiers, components of the information security organizations within the DIA, NGA, Air Force, Navy, and Army
- **Training Certifier**, component of the information organizations within the DoDIIS T&E located at the Defense Intelligence Analysis Center (DIAC)
- **NGA ITF** performs all aspects of testing as the JITF, JITC and IA

Management and User Communities:

- The DExA for the IMA
- PMOs
- Military Services and Unified Command System Integration Management Offices (SIMOs)
- Beta II test site and personnel
- DoDIIS IMA functional users.

The policies in this document describe key responsibilities necessary for the implementation of a successful Certification Process and should aid PMs 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 applications does not significantly change the life cycle process for IMAs 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; however, the objectives of each step shall be adhered to.

UNCLASSIFIED

Figure 1-1 provides a diagram of the DoDIIS IMA certification process. The steps in the certification process are defined by the DoDIIS Management Board (DMB) and are executed

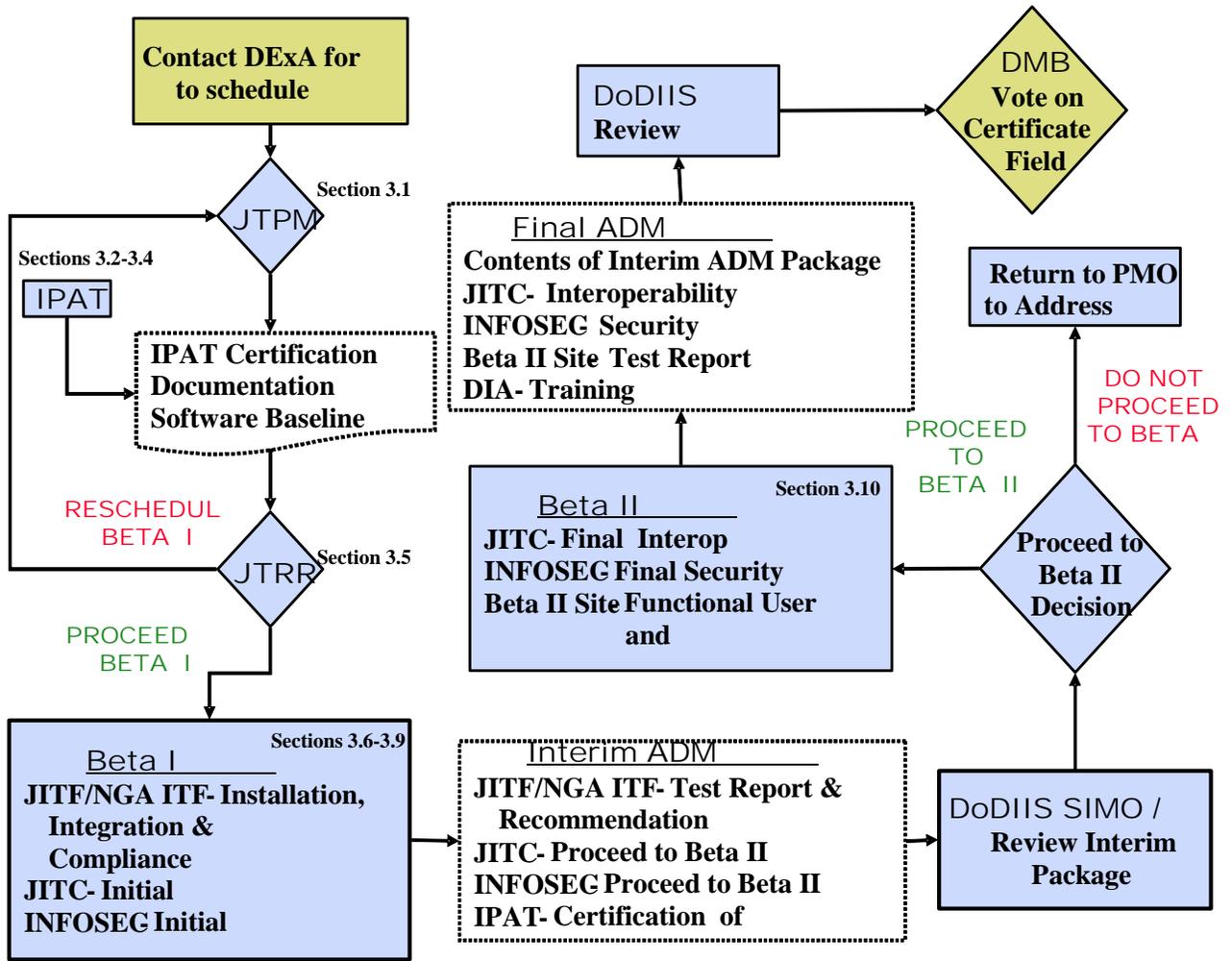


Figure 1-1 DoDIIS Certification Process

in coordination with the DExA for T&E to provide management oversight.

The DExA for Test and Evaluation is supported by the Test Agencies. Prior to DoDIIS IMA certification, the Program Managers (PM) 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 DoDIIS integration compliance requirements and security requirements, as tasked by the DMB.

Expertise, lessons learned and technology are shared between these functions. Test artifacts are available at the following sites:

UNCLASSIFIED

JITF Virtual Test Folder (VTF) site located on Intelink at <http://web1.rome.ic.gov/vtf>
Security Virtual Test Folder (SVTF) site on Intelink at <http://web1.rome.ic.gov/svtf>
JITC System Tracking Program (STP) site on NIPRNet at <https://stp.fhu.disa.mil/>
JITC Joint Interoperability Tool (JIT) site on NIPRNet at <http://jit.fhu.disa.mil/> or on
SIPRNet at <http://199.208.204.125/>

The net result of these feedback loops is to improve the overall process. Improvements will be implemented as updated integration requirements, revised documentation, tools, enhanced distribution technology and other products become available.

UNCLASSIFIED

UNCLASSIFIED

SECTION 2 - TEST AND EVALUATION OBJECTIVES

The overall goal of the DoDIIS 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 IMA T&E process is conducted to satisfy the following objectives:

- Support DMB milestone decisions and ensure user needs are met by validating the DoDIIS IMAs are thoroughly planned, understood and documented through a consistent test program. (Sections 3.1 – Joint Test Planning Meeting (JTPM))
- 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 IA testing. (Section 3.2 – In Plant Acceptance Testing (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 – Joint Test Readiness Review (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. (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 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 6/3 security requirements as applies to IMAs and user operations. (Section 3.8 –IA Testing)
- Determine, document and certify IMA interoperability and ability to function with other IMAs in an operational environment. (Section 3.10 - Beta II)

UNCLASSIFIED

UNCLASSIFIED

SECTION 3 - TESTING MILESTONES & EVENTS

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. Test artifacts are posted on the VTF and SVTF on Intelink. An index to the available test artifacts can also be found on the Internet.

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/Training/Beta II test activities
- Establishing a mutual understanding of the level of the **base lined** software release to be tested
- Ensuring all parties have a clear understanding of the certification process, requirements and the roles of test organizations
- Identifying the Beta II test site and verifying the Beta II Confirmation Letter (Appendix G).

The JTPM may be conducted as a meeting or via teleconference. A representative from all interested parties should attend the JTPM. The JTPM Scheduling Checklist found in Appendix D ensures all parties are ready for the JTPM. The following items govern coordinating, convening and follow-up of a JTPM:

- a. The PMO shall contact the DExA at least three months (90 days) prior to desired start of testing to schedule a JTPM.
- b. The PMO and the DExA for T&E will decide the location, date and time for the JTPM.
- c. The DExA for T&E 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 provide a completed IMA Profile in advance of the JTPM.
- e. The PMO shall have a representative at the JTPM.
- f. The DExA for T&E, or representative, shall chair the JTPM as moderator and assist in resolving issues where necessary.
- g. 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 form for the PMO to identify hardware, software and personnel requirements
 - Listing of required documentation and information
 - Self-assessment checklists

UNCLASSIFIED

- h. The JITF Work Plan form is provided to the IMA PMO prior to or at the JTPM. The PMO shall complete the Work Plan and return it to the JITF no later than forty-five (45) 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 by the DExA for T&E.
- k. The JITF shall post the JTPM Memo for Record (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 T&E shall serve as arbitrator when necessary.

A JTPM scheduled for a previously untested DoDIIS IMA or for one that has undergone major revision should be attended by representatives from:

- DExA for T&E
- JITF
- PMO, including a representative from the developer
- JITC
- GITC Training Representative (via message only)
- Applicable Agency/Service IA Certification organization
- IMA functional user community
- DoDIIS SIMO
- DoDIIS Engineering Review Board (ERB)
- PMO training Point of Contact (POC)

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

A MFR is published for posting on the VTF by the DExA for T&E, 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 (IPAT). Functional certification (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 T&E (electronic mail is acceptable) that the IMA has passed the IPAT. The IPAT certification letter shall include:
 - A statement the DoDIIS IMA functionality satisfied the Requirements Definition

UNCLASSIFIED

UNCLASSIFIED

Documentation and that all required functional capabilities are implemented and tested.

- A statement the 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. A critical point in the certification process is the delivery to the JITF of the software baseline.

- a. The IMA baseline shall be delivered to the JITF by mail or overnight express no later than fourteen (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 integration testing without the coordination of the JITF. The only changes that will be approved are to correct Impact Code 1 findings that can be remedied immediately to allow the continuation of testing.
- d. Any required 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. Appendix E contains a checklist of the documentation and information to be provided by the IMA PMO, associated due dates, and the organizations requiring this information.

The following table (page 13) identifies the types of documentation to be provided by the PMO to the Test Agencies (JITF, JITC, IA and Training). This listing is not comprehensive and not all documents are required by all IMAs. Documents and information not on the list but deemed necessary for testing shall be identified in consultation between PMO and the Test Agencies.

UNCLASSIFIED

UNCLASSIFIED

Document Type	Information Content
<i>Requirements Definition Documentation</i>	Provides written requirements for the IMA
<i>Requirements Traceability Matrix</i>	Traces requirements through program Documentation
<i>Security Accreditation Documentation</i>	Provides information in accordance with the DoDIIS Certification and Accreditation Guide for Automated Information Systems (AIS) Security in Intelligence Information Systems and the DCID 6/3
<i>Test Plans, Procedures and Test Reports</i>	Provides information as described in IEEE /EIA Standard 12207
<i>Interface Control Document</i>	Provides detailed information on interfaces between applications
<i>Software Version Description</i>	Provides information regarding the software version, including changes and known problems
<i>User Documentation</i>	Users manuals, operator guides
<i>Run Time Interface Document</i>	Provides detailed software configuration information
<i>Configuration and Installation Guide</i>	Provides software installation instructions
<i>Transition Plans</i>	Transition details for software upgrades, database changes, future direction for requirements and design of software application
<i>Open Problem Reports</i>	Descriptions of all open problem reports against the version undergoing testing
<i>Training Management Plan</i>	Identifies training planned for the IMA

3.5 Joint Test Readiness Review (JTRR). The JTRR is to be conducted five to ten business days 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. A checklist of mandatory topics to be covered in the JTRR is located at Appendix F.

- a. The JTRR mandatory agenda items checklist found in Appendix F shall be used as the basis of the JTRR.
- b. At the conclusion of the JTRR, the JITF shall provide the DExA for T&E notification (e-mail dexa.te@langley.af.mil or FAX is acceptable) that all requirements to begin testing have been met or if there are any outstanding issues that must be resolved.

The PM must obtain verification from the JITF that all required documentation has been provided or satisfactory arrangement with the JITF to obtain the required documentation has been made. Failure to provide the required documentation will result in cancellation of the scheduled test. When the required documentation is provided to the JITF, the testing can

UNCLASSIFIED

proceed. In the event of cancellation, the DExA for T&E shall coordinate with the testing components and the PM on a new test date.

3.6 JITF Testing. The JITF conducts installation, integration and security vulnerability testing in support of the DMB, user sites, and PMOs. JITF testing is normally conducted at the Air Force Research Laboratory (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, Commercial Off The Shelf (COTS) and Government Off The Shelf (GOTS) found at operational sites. This robust environment allows the JITF to simulate commonly used business practices as identified by DoDIIS users. When required the JITF will also conduct tests at offsite locations.

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 and infrastructure compliance testing are mandated in the *DoDIIS Instructions*, Section 4.1. A positive evaluation of an IMA during integration testing is based in large part on the extent that the IMA meets the integration requirements that are documented in the JITF/National Imagery and Mapping Agency (NIMA) Integration Test Facility (ITF) *DoDIIS Integration Requirements and Evaluation Procedures Version 4.2*, published by the JITF. (***Please note that NIMA has changed to NGA***). The integration requirements identify technical areas of software installation, configuration and use that influence 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 integration 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.
- Integration Security – These objectives identify areas of the design and operation of the application that may affect the site security architecture and include a VA of the

UNCLASSIFIED

UNCLASSIFIED

IMA. 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. Integration requirements are published by the JITF 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/>. For each requirement that the IMA does not meet, the JITF documents a finding and assesses an impact level.

Not all integration requirements have equal weight. 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 requirements they do not meet. The following describes the levels of impact findings.

JITF Impact Code description as identified in the *JITF/NIMA ITF DoDIIS Integration Requirements and Evaluation Procedures version 4.2* and JITF test reports are listed below.

Impact Code 1

A finding that,

- a) identifies baseline adjustments, not included in the installation guide, made during the test event in order to successfully install the application;
- b) has a serious effect on the operation of either the application or on another application or component of the infrastructure; or
- c) impacts cost, schedule, performance or Post-Deployment Software Support (PDSS).
- d) identifies a security vulnerability in the application or site architecture that can be exploited by a general user; or
- e) seriously increases the level of effort required by site personnel to manage the application or other applications.

An Impact Code 1 finding is assigned if the application baseline must be changed in order to continue testing, if the installation documentation is not detailed enough to support the successful installation of the application, or if a security vulnerability exists.

The level of effort is a key determinant for Impact Code 1 findings. The time or expertise that is required to install or manage the application cannot exceed what is reasonably expected for an application. For example, if the installation guide says that the application can be installed in a single day, but the installation takes more than 20 working hours, then an Impact Code 1 finding would be generated.

An application cannot proceed to Beta II testing until all Impact Code 1 findings have been resolved by the PMO and verified by the JITF Engineers.

Impact Code 2

A finding that,

- a) has a significant effect upon, but does not prevent, the successful installation of the application under evaluation;
- b) has a significant effect on the operation of either the application or on another application or component of the infrastructure;

UNCLASSIFIED

UNCLASSIFIED

- c) impacts cost, schedule, performance or Post-Deployment Software Support (PDSS).
- d) creates a security vulnerability in the application; or
- e) significantly increases the level of effort required by site personnel to manage the application or other applications.

An Impact Code 2 finding can be resolved by a change in procedure or configuration. The resolution of an Impact Code 2 finding requires a significant level of effort by site administrators. The resolution does not cause significant delay in integration testing; instead, it can be proposed and evaluated during integration testing at the JITF or NIMA ITF.

Impact Code 2 findings do not cause integration test failure, but the accumulation of Impact Code 2 findings may affect the test organization's "go/no go" recommendation.

Impact Code 3

A finding that,

- a) has an effect upon the installation of the application under evaluation;
- b) has a effect on the operation of either the application or on another application or component of the infrastructure; or
- c) increases the level of effort required by site personnel to manage the application or other applications, but does not require a significant level of effort by site administrators.

The successful resolution of an Impact Code 3 finding requires technical expertise expected of site administrators. The resolution does not cause significant delay in integration testing; instead, it can be proposed and evaluated during integration testing at the JITF or NIMA ITF.

Impact Code 3 findings do not cause integration test failure, but the accumulation of Impact Code 3 findings may affect the test organization's "go/no go" recommendation.

Impact Code 4

A finding that,

- a) has little or no effect upon the installation of the application under evaluation;
- b) has a little effect on the operation of either the application or on another application or component of the infrastructure; or
- c) nominally increases the level of effort required by site personnel to manage the application or other applications, but does not require a significant level of effort by site administrators.

The finding can be resolved by a workaround that can be implemented as a change in during integration testing without a significant level of effort, or the finding can be left as is. Even though the finding has some effect on the configuration or operation of the mission application, or on other components of the site architecture the administrator will be able to manage the mission application.

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 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:

UNCLASSIFIED

UNCLASSIFIED

- 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. - Seventy-five (75) percent of applicable integration requirements are met – The goal of integration 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. Passing fewer than seventy-five (75) percent of applicable requirements 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 3. - There are no open Security Category I or II findings as a result of the VA conducted by the JITF
- ITEM 4 - Security documentation will be available on the SVTF located on Intelink at <http://web1.rome.ic.gov/svtf>

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 Information Management Services Configuration Management (IMS 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 (5) working days after completion of JITF testing. The PMO and DExA have two (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 in writing using the Configuration Management Data Base (CMDB) to generate Document Review Reports (DRRs). The CMDB is available on the Non-Secure Internet Protocol Routing NETWORK (NIPRNET), Secret Internet Protocol Routing NETWORK (SIPRNET) and Joint Worldwide Intelligence Communication System (JWICS) networks. Accounts can be arranged upon request.
- c. The JITF shall distribute the final test report to the DExA for T&E, DMB, DoDIIS SIMO, ERB, and PMO ten (10) working days after completion of JITF testing.
- d. The JITF shall post the final test report on the VTF after release to the PMO. An annex containing the results of the VA will be posted on the SVTF.

The final report shall contain a recommendation to proceed to certification based on the criteria set forth in Appendix J and based in large part on the extent the IMA meets the integration requirements documented in the *JITF/NIMA ITF DoDIIS Integration Requirements and Evaluation Procedures*.

3.7 JITC Testing. The JITC is responsible for certifying that all Department of Defense Command, Control, Communications, Computers and Intelligence (C4I) systems are interoperable. Department of Defense Directive 4630.5 "Interoperability and Supportability

UNCLASSIFIED

UNCLASSIFIED

of Information Technology and National Security Systems" [January 11, 2002] and Department of Defense Instruction 4630.8 "Procedures for Interoperability and Supportability of Information Technology and National Security Systems" [May 2, 2002] mandate joint and combined interoperability certification testing for "all Command, Control, Communications and Intelligence (C3I) systems developed for use by US forces." This certification must be obtained prior to fielding a new system. Concerning the DoDIIS test process the JITC test directors will:

- Extract interoperability requirements from system documentation and through interviews with the system PMO, system developer and potential users. Based on J6 [Joint Staff] approved joint interoperability or user-defined requirements, develop a Draft Interoperability Test Plan.
- Coordinate with the JITF or PMO to determine the required interfaces that will be available during Beta I testing. The JITC participates in the JITF JTRR approximately two (2) weeks prior to the Beta I test. JITC testers will identify shortfalls between requirements and test events to include any test limitations.
- Observe Beta I test events or review results and collect data pertinent to interoperability.
- Develop specific interoperability test events to be conducted at the Beta I test, based on the Draft Interoperability Test Plan and systems availability.
- Validate the Draft Interoperability Test Plan with the PM or their designated representative.
- Upon successful completion of the Beta I test, JITC will develop the final Interoperability Test Plan and provide a recommendation memorandum to the DMB based on the criteria below:
 - **Recommend Proceed.** Recommend proceed indicates the IMA meets ALL or SOME of the joint interoperability requirements defined by the users and the unmet requirements will result 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.
 - **Recommend Conditional Proceed.** Recommend conditional proceed indicates the IMA meets SOME of the joint interoperability requirements defined by the users, and the unmet requirements will result in MAJOR 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 only if the unmet requirements are scheduled for prompt resolution within six (6) months.
 - **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 will result 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.

UNCLASSIFIED

UNCLASSIFIED

- Conduct joint interoperability testing at an operational location identified by the PMO at the Beta II test event. Work with operational users to determine if approved J6 joint interoperability or user-defined requirements are met. Based on test results, prepare an Interoperability Test Report and Interoperability Assessment or Joint Interoperability Certification memorandum. The JITC goal is to publish the Interoperability Assessment or Joint Interoperability Certification memorandum and forward it to the DMB within fourteen (14) days after Beta II testing is completed. The Interoperability Test Report should be completed within thirty (30) days after Beta II testing is completed.

3.7.1 Interoperability Test Execution. The focus of interoperability testing is on the ability of systems to securely exchange information in sufficient time, by the designated communications means, with the accuracy required by the user to perform assigned missions. Criteria in the templates may have to be adjusted to ensure this can be tested adequately based on the requirements of the system under test. Most initial interoperability testing of DoDIIS IMAs will be conducted at the JITF. By a Memorandum of Agreement (MOA) with the JITF, the JITC will conduct its testing and draft test plan validation during integration testing (Beta I). Follow-up testing in an operational environment is conducted at various operational DoDIIS Sites (Beta II testing) around the world. The JITC documents the results of interoperability testing in Test Reports and Interoperability Assessments or Joint Interoperability Certification memorandums used by the DMB to support interim fielding decisions.

3.7.2 Interoperability Test Certification. The JITC tests DoDIIS IMAs for joint interoperability and certification in accordance with the guidelines by JITC and Joint Interoperability and Engineering Organization (JIEO) Circular 9002 "Requirements Assessment and Interoperability Certification of C4I and AIS Equipment and Systems." The tests determine the interoperability of DoDIIS IMAs with other DoDIIS, Joint and Service systems. Most DoDIIS applications are AIS designed for network services and for the exchange of message traffic or textual information, imagery products and databases. Based on the overall results of the DoDIIS testing process (documentation review, developer interviews, and Beta test events) the JITC will issue one of the following:

- Full System Certification - System meets all J6 approved joint interoperability requirements
- Specified Interfaces Certification - System meets subset of the J6 approved joint interoperability requirements
- Non-Certification - System is fielded, critical operational impacts expected. This memorandum provides a warning to the Warfighter about systems non-certification
- Interoperability Assessment - System does not have J6 approved joint interoperability requirements so user-defined requirements are used or customer requests JITC to assess whether interoperability testing is needed for the system

3.8 Information Assurance (IA) (Security) Testing. IA Certifiers (IAC) include DIA, Air Force, Army and Navy Security representatives. IACs are responsible for validating DCID 6/3 security requirements In Accordance With (IAW) Mode of Operation, testing

UNCLASSIFIED

UNCLASSIFIED

interoperability with the DoDIIS infrastructure, validating Security Concept of Operations (SECONOPS) and testing user efficiency/training as it relates to security.

3.8.1. IA Test Architecture. All security testing will be completed on the specific DoDIIS IMA suite of equipment installed at the JITF or Beta II sites. IA testing may also occur at the PMO/Contractor site.

3.8.2. IA 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 6/3, Joint DoDIIS Cryptologic SCI (Secure Compartmented Information) Information Systems Security Standards (JDCSISSS) and DIA Manual (DIAM)50-4. System accreditation documents (Concept of Operation (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 conducted in conjunction with testing at the JITF and at the Beta II site.

- a. IACs shall test the following:
 - System Discretionary Access Controls
 - Audit Capabilities
 - User ID/Authentication
 - Data Integrity
 - System Integrity
 - Data Labeling
- b. The IACs 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., four (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.

3.8.3 Generation and Distribution of Findings. The information generated by the IA 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 IAC's recommendation on IMA security status.

- a. The PMO shall present the Security Certification Letter to the Beta II site Information

UNCLASSIFIED

UNCLASSIFIED

and has consideration been provided to integrate such training into functional intelligence course(s)?

Results of Training Certification will be posted on the VTF (Intelink) web site <http://web1.rome.ic.gov/vtf>.

3.10 Beta II Testing. Upon DoDIIS SIMO approval, the PMO proceeds to the Beta II test site(s). Beta II testing validates the IMA's functionality and stability in an operational environment. The focus of Beta II testing is to assess the application's operational effectiveness, user efficiency, suitability and determine the impact on the security architecture, and ensure interoperability. Beta II IA and interoperability test results are reported by the IAC and the JITC respectively, which provide their formal certifications. The Beta II test report is produced by the host Command and distributed to the DoDIIS SIMO and the PMO.

Note: The PMO shall not make any modifications to the baseline tested unless those changes were identified and agreed to by the testing agencies.

Additionally Beta II testing is to certify IMA IA, interoperability and functionality with other IMAs or AISs in an operational environment. The Beta II testing environment most closely represents an operational environment which is important to the certification process for the IA and interoperability testing. The PMO is charged with the responsibility for preparations for the Beta II test.

The principle objectives of Beta II are to:

- Validate the IMA works in an operational environment
 - Ensure problems encountered during Beta I are cleared
 - Verify the IMA meets DCID 6/3 security requirements in an operational environment
 - Interoperability requirements are met
- 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

3.10.1 Beta II 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. The Beta II test site(s) should be identified prior to and confirmed at the JTPM to allow participation of the host site in planning activities.

Note: The DExA for T&E must receive a Beta II Confirmation Letter from the PMO before

UNCLASSIFIED

UNCLASSIFIED

certification testing components will proceed to a Beta II site.

- a. The PMO will choose Beta II site(s) that best represent the operation of the IMA within the user community and will get written confirmation from the Beta II Site Commander allowing the test to be performed at their site. The format for the confirmation letter is found in Appendix G. This confirmation letter shall be forwarded to the DEXA for T&E prior to Beta I testing. Specific site selection considerations include:
 - Volunteer
 - Prime user of IMA undergoing Beta II testing
 - Maximum number of interfacing systems on site
 - Maximum number of supported platforms
 - Participant in system development process
 - Availability of facilities and personnel
 - Active in review and update of test plans and procedures
- b. JITC interoperability testers and IACs will participate in Beta II site tests. JITF may also be present for observation and/or participation in Beta II testing. 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. The PMO and Beta II site may want to include local tester personnel in addition to the site operators to ensure more exhaustive and robust Beta II testing.

3.10.2 Beta II Preparations. Appendix G provides a recommended resource checklist for Beta II sites. As part of the preparations for Beta II Testing:

- a. Based on the Beta II site selection criteria in the previous section, the PMO shall identify the Beta II test site prior to the JTPM.
- b. The PMO shall be responsible/oversee the IMA software installation at the Beta II site.
- c. The PMO shall be responsible for getting the Beta II Site Commander's authorization for testing and provide a signed Beta II Confirmation Letter. The confirmation letter format can be found in Appendix G.
- d. The IMA shall be installed at the Beta II site by following the installation plan published by the PMO and validated at the JITF.
- e. The PMO shall coordinate a Beta II site for verifying the functionality of the application.
- f. The Beta II site personnel shall develop operational scenario testing procedures based on anticipated operational use of the application.

3.10.3 Beta II Activities. 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 follow.

UNCLASSIFIED

UNCLASSIFIED

- a. The Beta II Site shall obtain site authorization, coordinating requirements, and ensuring resource scheduling using the Beta II Site Confirmation Letter Memorandum located in Appendix G.
- b. The Beta II Site shall complete the security site accreditation package prior to testing, i.e., written site/command ISSM approval is needed before the IMA is added to the test site.
- c. The Beta II Site shall document the results of the Beta II test using the Beta II Test Report format located in Appendix G.
- d. The Beta II Site shall assign at least one System Administrator, an ISSO and one functional user to support and participate in Beta II testing and in any post-Beta II testing to validate implementation of any corrections to Beta II findings.
- e. The Beta II Site shall provide test results to the PM for inclusion in the ADM package within two weeks after completion of testing. 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/Life Cycle Management (LCM) at the DoDIIS SIMO 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.
- f. In the event a change occurs to the application baseline after Beta II testing, a Beta II Site Representative will participate in any PMO testing to validate implementation of Beta II findings.
- g. The PMO and JITC shall coordinate with the DExA activities relating to interoperability testing at the Beta II Site
- h. The JITC shall plan interoperability events to be conducted at the Beta II
- i. The JITC shall collect interoperability data from the Beta II site and identify interoperability shortfalls
- j. The JITC and IACs will conduct necessary testing to complete test objectives identified during the JTPM
- k. The JITC shall, upon successful completion of the Beta II, produce a Joint Interoperability Certification/Assessment memorandum (combining the results from both Beta I and II testing) for the DMBs final fielding decision.
- l. The IACs shall, upon successful completion of the Beta II, produce a detailed test report to the DoDIIS SIMO and PM.
- m. The JITF, on a case by case basis, will attend Beta II to confirm Beta I results and provide support.
- n. The JITF will post the Beta II Test Report to the VTF.

UNCLASSIFIED

UNCLASSIFIED

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 overseeing the DoDIIS T&E Program as chartered by the DMB. The DExA is committed to improving the quality and usability of DoDIIS IMAs in support of the Combatant Commands. Specifically, the DExA for T&E 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 affectivity date of each individual document.
- c. Preparation and execution of the DoDIIS T&E budget.
- d. Serving as Chair/host for JTPMs and determining PMO readiness to proceed to test by the time of the JTRR.
- e. Participating in DoDIIS meetings related to JITF and JITC T&E.
- f. Acting as the primary interface between DoDIIS community and the Test Agencies.
- g. Acting as a liaison between Testing Agencies and PMO organizations to mediate concerns and 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:

UNCLASSIFIED

- 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:
 - Distributed integration and interoperability testing
 - Site business practice concerns such as user interfaces, application interfaces and other 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 provides access to the DoDIIS Community all IMA test reports, MFRs (minutes) of JTPMs, TPOC information and other test related information including reviews of minor and maintenance releases.

The VTF is administered by the JTIF under oversight of the DExA for T&E. The JTIF is responsible 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.rl.af.mil/jitf/> or Intelink <http://web1.rome.ic.gov/vtf>

4.6 Security Virtual Test Folder (SVTF). The SVTF provides access to the IMA's VA reports, as annexes to the JTIF Test Report, and Draft and Final Security packages. Security documentation on the SVTF provides an authoritative source for Beta I and Beta II testers, as well as ISSMs. The SVTF is implemented similarly to the VTF with the added requirement for login access. The accounts for the SVTF are setup through the respective Security Certification Offices (SCOs). The SVTF is located on Intelink at: <http://web1.rome.ic.gov/svtf>.

4.7 Distributed Testing Network (DTN). The DExA for T&E encourages use of the DTN as a means of conserving resources by using connectivity provided by the JWICS or collateral networks, where available. When warranted, testing may occur using 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.af.mil/jitf/> or Intelink <http://web1.rome.ic.gov/vtf>.

4.8 Testing Configuration Management (CM). The T&E Policy for CM is summarized in the following.

- a. The existing IMS CM process shall support the testing CM requirements and shall be the central repository for submitted test findings including software and document test findings

UNCLASSIFIED

UNCLASSIFIED

and action items. IMS CM uses the CMDB to log, track and monitor all test findings, supporting documentation and software, and test reports.

b. All test findings written during the testing process by the JITF, JITC, 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.

Further information about IMS CM and the CMDB is available through the Internet <http://www.if.afrl.af.mil/programs/jitf/> or Intelink <http://web1.rome.ic.gov/vtf>.

4.9 Test Organizations

4.9.1 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 application 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. Performs Installation/De-installation verification.
- c. Performs DoDIIS Integration Testing.
- d. Supports testing at user sites, JITC and Security testing, as required.
- e. Conducts VAs in support of DIA/SYS4.
- f. Provides lessons learned or other assistance to DoDIIS PMOs and developers as needed or requested.
- g. Provides technical support and information to user sites as required.
- h. Provides a JITF DTN for integration testing.
- i. Under the oversight of the DExA for T&E, the JITF shall also
 - Review and take action to retest (if necessary) all other DoDIIS IMA deficiencies reported by DoDIIS users that may have been missed during the testing cycle.
 - 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 dexa.te@langley.af.mil) or FAX or by memo.
 - Review minor, maintenance, and patch releases to determine the need for testing, and provide a go/no go recommendation to the DoDIIS SIMO/LCM concerning readiness to field.

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

UNCLASSIFIED

UNCLASSIFIED

4.9.2 Joint Interoperability Test Command (JITC). Interoperability consists of determining the ability of a system to securely 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 securely 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.

The JITC provides interoperability status information via the JITC STP accessible to .mil/.gov users at NIPRNET: <https://stp.fhu.disa.mil/>. Test reports, lessons learned, and related testing documents and references are on the JITC JIT at NIPRNET: <http://jit.fhu.disa.mil/> and SIPRNET: <http://199.208.204.125/>

4.9.3 Information Assurance (IA) Accreditation Certifiers. The IA Accreditation Certifiers are from the security offices of the DIA, NSA, 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 SCO (Army, Navy, or Air Force) and the Site 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.

4.9.4 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. Complying with the DMB directed DoDIIS IMA Version Release Policy in Appendix I of this document.
- c. Selecting Beta II site(s) according to selection criteria listed in Appendix G of this

UNCLASSIFIED

UNCLASSIFIED

document.

- d. Scheduling the JTPM with the DExA. (At this time, the PMO should have selected a Beta II site and notified the Site personnel of the scheduled JTPM.)
- e. Participating in the JTPM.
- f. Distributing all base-lined application documents to testing agencies for comment in accordance with timelines established in Appendix E. If required documentation is not provided, the scheduled test will be postponed or cancelled until documentation can be produced. New test dates will be scheduled by the DExA for T&E in consultation with the test components.
- g. Completing the Interface Control Document. Suggested format can be found in the Interface Requirement Specification (IRS) in MIL- STD 498, DID Number DI- IPSC- 81434 as the standard format. (MIL-STD 498 was cancelled effective 27 May 98; however, the DIDs remain in effect.)
- h. Completing a configuration and installation guide. Suggested format can be found in the Software Installation Plan (SIP) in MIL-STD 498, DID Number DI- IPSC- 81428 as the standard format.
- i. Subscribing to or linking to the VTF and the SVTF.
- j. Inviting Test Agencies to witness IPAT conducted by the developer.
- k. Conducting functional testing.
- l. Submitting an IPAT Functional Certification Letter to JITF/JITC according to requirements in Section 3.2 of this document.
- m. 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. 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.
- n. Preparing and sending an ADM to the DoDIIS SIMO office IAW the *DoDIIS Instructions* and DIA Regulation 65- 13.
- o. Submitting the PMO Security Certification Letter to the Beta II site ISSM/ISSO, prior to the Beta II test. (Appendix H)
- p. Coordinating Beta II testing at an operational site with the ISSO/ISSM and DoDIIS SIMO.
- q. Coordinating system developer support at Beta II testing, if necessary.
- r. Updating the ADM after Beta II testing.
- s. Validating the implementation or approval of changes to the baseline based on Beta II findings with Beta II representative participation/coordination.

UNCLASSIFIED

UNCLASSIFIED

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. IMS CM (<http://www.rl.af.mil/programs/ims>) (NIPRNET) 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 thirty (30) days after publication unless otherwise directed.

Two other NIPRNET URL sites may be used.

<http://www.rl.af.mil/programs/jitf>

<http://www.rl.af.mil/jitf>

UNCLASSIFIED

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.

Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01C, Interoperability and Supportability of National Security Systems, and Information Technology Systems, June 2003.

Director of Central Intelligence Directive (DCID) 6/3, “Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks”, 5 June 1999.

Defense Intelligence Agency Manual (DIAM) 50-4, Department of Defense Intelligence Information System (DoDIIS) Information Systems Security (Information Assurance (IA)) Program, 30 April 1997

Defense Intelligence Agency Regulation 24-11, General Intelligence Training System (GITS)

Defense Intelligence Agency Regulation 65-13, Automated Information System Life Cycle Management

Department of Defense (DoD) Directive 3305.2, “DoD General Intelligence Training”, 20 July 1984

Department of Defense (DoD) Directive 4630.5, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), 11 January 2002.

Department of Defense (DoD) Directive 5000.1, "Defense Acquisition System", 12 May 2003

Department of Defense (DoD) 5000.2-R, Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs, 5 April 2002

Department of Defense (DoD) Directive 5200.28, “Security Requirements for Automated Information Systems (AISs)”, 21 March 1988

Department of Defense (DoD) Directive 8320.1-M, DoD Data Administration, March 1994

Department of Defense (DoD) Joint Technical Architecture (JTA), Version 5.0, 4 April 2003

Department of Defense (DoD) Architecture Framework, Version 3.0, 30 August 2003

Department of Defense Intelligence Information System (DoDIIS) Site Certifier’s Guide, SC-2610-143-93, November 1993

IEEE/EIA 12207 – Information Technology – Software Lifecycle Processes, 1 Aug 1995

UNCLASSIFIED

UNCLASSIFIED

Department of Defense Intelligence Information System (DoDIIS) Security Architecture Guidance and Directions

DoDIIS Certification and Accreditation Guide for Automated Information Systems (AIS) Security in Intelligence Information Systems, DS 2610-142-01

DoDIIS Instructions 2000, February 2000

DoDIIS T&E Information Package

DoDIIS Test Process Oversight Committee (TPOC) Charter, 13 February 1997

DoDIIS Integration Requirements and Evaluation Procedures (*in JITF Homepage*)

Joint Integration Test Facility (JITF), Virtual Test Folder (VTF) Concept of Operations, 9 March 1999

Joint Integration Test Facility (JITF), Distributed Test Network (DTN) Concept of Operations, January 1998

Joint Interoperability Test Command (JITC) Instruction 210-85-01, Documentation of Test and Evaluation Activities

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 IMAs Test, and the DoDIIS Joint Integration Test Facility (JITF); "Interoperability Test and Certification of DoDIIS IMAs", 19 November 1995

Joint Integration Test Facility/Joint Interoperability Test Center/DoDIIS Management Board Memorandum of Understanding, October 1995

Justification and Remarks for Joint Integration Test Facility, Joseph D. Baldino, Chief, Systems Analysis, DIA, Washington DC, 15 June 1995

Air Force Research Laboratory, Information Management Services (formally Common User Baseline for the Intelligence Community (CUBIC)) Configuration Management Plan, 9 August 2001

UNCLASSIFIED

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 an IMA or network is approved to operate. Details on security guidance for IMAs can be found in the *DoDIIS Certification and Accreditation Guide for Automated Information Systems (AIS) Security in DoD Intelligence Information Systems*.
- **Client process** – Client processes make requests for service from server processes (see Server definition). 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.
- **Information Management Services (IMS)**– A standard set of IMS and CM processes used to facilitate communication, to log, track and monitor critical information between users, PMOs and the Test Agencies.
- **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 a 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.
- **Server** – Workstations (definition 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. In addition, browser applications will be stored for client retrieval.

UNCLASSIFIED

- **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 containing all test process information to facilitate the Command feedback portion of the DoDIIS IMAs 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
 - Beta II test results
- **Security Virtual Test Folder (SVTF)** - A website maintained by the JITF containing IMA's Vulnerability Assessment (VA) Reports, Draft and Final Security packages. Security documentation on the SVTF provides an authoritative source for Beta I and Beta II testers, as well as ISSMs. The SVTF is implemented similarly to the VTF with the added requirement for login access. The accounts for the SVTF are setup through the respective Security Certification Offices (SCOs).

UNCLASSIFIED

UNCLASSIFIED

APPENDIX C - ACRONYMS AND ABBREVIATIONS

This listing covers the main text and the Appendices.

ADM	Acquisition Decision Memorandum
AFRL	Air Force Research Laboratory
AIS	Automated Information System
CCBs	Configuration Control Boards
CONOPS	Concept of Operations
COTS	Commercial off the Shelf
CM	Configuration Management
CMDB	Configuration Management Data Base
CONOPS	Concept of Operations
CR	Change Request
CUBIC	Common User Baseline for the Intelligence Community
DCID	Director Central Intelligence Directive
DExA	DoDIIS Executive Agent
DIA	Defense Intelligence Agency
DIAC	Defense Intelligence Analysis Center
DIA/DR	Director of the Defense Intelligence Agency
DIAM	DIA Manual
DISA	Defense Information Systems Agency
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
GITC	General Intelligence Training Council
GOTS	Government off the Shelf
IA	Information Assurance
IAC	Information Assurance Certifier
IAW	In Accordance With
IC	Intelligence Community
ICD	Interface Control Document
IMA	Intelligence Mission Application
IMS	Information Management System
IPAT	In-plant Acceptance Testing
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
ITF	Integration Test Facility
ITMRA	Information Technology Management Reform Act (of 1996)
JDCSCISS	Joint DoDIIS Cryptologic SCI (Secure Compartmented Information) Information Systems Security Standards
JIEO	Joint Interoperability Engineering Organization
JIT	Joint Interoperability Tool
JITC	Joint Interoperability Test Command

UNCLASSIFIED

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
LCM	Life Cycle Management
MFR	Memorandum for Record
MOA	Memorandum of Agreement
NGA	National Geospatial-Intelligence Agency (formerly NIMA)
NIMA	National Imagery and Mapping Agency
NIPRNET	Non-Secure Internet Protocol Routing NETWORK
NLT	No Later Than
PAA	Principal Accreditation Authority
POC	Point of Contact
POI	Program of Instruction
PM	Program Manager
PMO	Program Management Office
S&T	Scientific and Technical
SCO	Service Certifying Organization
SECONOPS	Security Concept of Operations
SIMO	System Integration Management Office
SIPRNET	Secret Internet Protocol Routing NETWORK
STP	System Tracking Program
SVTF	Security Virtual Test Folder
T&E	Test and Evaluation
TPOC	Test Process Oversight Committee
VA	Vulnerability Assessment
VTF	Virtual Test Folder

UNCLASSIFIED

APPENDIX D – JOINT TEST PLANNING MEETING (JTPM) SCHEDULING CHECKLIST

System: _____

Note: It may be beneficial to email or fax a copy of this first section (1) checklist to the PM and have them complete it, email or fax it back, then discuss any questions.

1. When PMO calls to schedule a JTPM, gather the following information:
 - a. System Name and Version Number: _____
 - b. Is the system applying for Initial Certification or Re-Certification?
 - c. What is the requested date and location for the JTPM? _____
 - d. What are the anticipated Beta I dates: _____
 - e. Security Testing:
 - 1) Who: __DIA __USAF __USA __USN __NGA
 - 2) When: _____
 - 3) Where (Will JITF systems be used?): _____
 - f. Interoperability Testing:
 - 1) What are the program interfaces? _____
 - 2) Are any of these new interfaces? _____
 - g. Beta II:
 - 1) What site has agreed to host Beta II: _____
 - 2) Beta II POC name and phone: _____
 - 3) If PM does not have a Beta II site yet, encourage them to have it prior to JTPM.
 - h. Training Management Plan has been sent to the GITS or CITC POC:

 - i. PM to have a short briefing, point paper, or synopsis on this program, its changes and interfaces (if JTPM is to be conducted as an attended meeting). Otherwise, PM should email or fax an unclassified synopsis of the program to principal participants prior to the JTPM conducted via video teleconference or teleconference.
 - j. PM (or PM's assigned lead): _____
Phone: _____ E-mail Address: _____

Note to JTPM Coordinator: These items can be discussed at the JTPM. Make sure the PM knows we are looking for representation at the meeting from these agencies.

UNCLASSIFIED

- 2. If necessary, reserve facilities for the JTPM.
- 3. Contact the JITF Representative and:
 - a. Advise JITF Rep of JTPM date.
 - 1) Pass requested JITF dates.
 - 2) If JITF cannot support those dates, the DExA will coordinate with the PMO new dates.

b. Verify JITF JTPM attendance.

JITF Rep: _____ Phone: _____
E-mail Address: _____

- 4. Contact the JITC Representative to
 - a. Determine if rep can attend JTPM. YES or NO
 - b. Verify interfaces to be tested.

JITC Rep: _____ Phone: _____
E-mail Address: _____

- 5. Contact Security Representative and verify JTPM attendance. YES or NO

Security Rep: _____ Phone: _____
E-mail Address: _____

- 6. Contact Training Representative and verify JTPM attendance. YES or NO

Training Rep: _____ Phone: _____
E-mail Address: _____

- 7. Send out a confirmation email to all agencies involved in the test.
- 8. Are there additional participants PM would like us to notify? If so, the PM is to provide names, phone number & email address.

UNCLASSIFIED

APPENDIX E - JTPM MEMORANDUM FOR RECORD

(Date)

FROM: AFC2ISRC/INYE, DoDIIS Executive Agent for Test and Evaluation (DExA for T&E)

SUBJECT: Joint Test Planning Meeting (JTPM) for XXXX version x.x

1. **PURPOSE:** To determine the testing schedule for the xxx version x.x

2. **DATE OF JTPM and LOCATION:** The JTPM was held on (date) at (location).

3. PARTICIPANTS:

<i>Representing:</i>	<i>Name:</i>	<i>Office/Organization</i>	<i>Phone:</i>	<i>Unclassified E-mail:</i>
DExA for T&E			Comm: DSN xxx	
			Comm: DSN xxx	

UNCLASSIFIED

1. CERTIFICATION SUMMARY

Type of Release:	(Major/Minor)
Scope of Change:	
In-plant Acceptance Testing:	Date: POC:

2. GENERAL COMMENTS:

- a. DExA for T&E:
- b. Program Representative:
- c. JITF Representative:
- d. JITC Representative:
- e. Security:
- f. Training Coordination:
- g. Beta II:

3. OUTSTANDING ISSUES FROM JTPM :

- a. The PM Representatives will:
- b. The JITC Representative will:

7. POC FOR THIS MEMO:

DExA at (757) 225-2910 or DSN 575-2910
E-mail: dexa.te@langley.af.mil

//signed//
DExA, USAF
DoDIIS Test & Evaluation Operations
Integration & Systems Branch

Atchs

- 1. DoDIIS Testing Timeline

UNCLASSIFIED

Event	Date (dd mmm yy)	Remarks
Joint Test Planning Meeting (JTPM)		Scheduled with the DExA ninety (90) days prior to Beta I testing
Documentation Due to Security Request for Certification Ltr (Appendix H) SSAA (Appendix D from C&A Guide) SRTM, TFM, and Test Procedures		Due at JTPM
		Due at JTPM
		Due sixty (60) days prior to Beta I testing
Interface & Req'ts Docs Due to JITC		Due at JTPM.
IMA Profile		Due at JTPM
Request for Training Certification		Due fourteen (14) days following JTPM. E-mail to training certifier.
New/updated Training Management Plan		Due sixty (60) prior to Beta I testing.
JITC Draft Test Plan		Thirty (30) days prior to Beta I testing.
Beta II Site Coordination Letter		Thirty (30) days prior to Beta I testing.
Workplan Due to JITF		Forty-five (45) days prior to Beta I testing.
Documentation Due to JITF		Fourteen (14) days prior to Beta I testing.
IPAT		To be completed prior to JTRR.
Pre-test Review (If applicable) Workplan Documentation Pre-test telecon		Pre-test review can be scheduled separate from IPAT and can be in the form of a documentation review, software pre-look or combination of the two. If a pre-test is desired, the following dates must be established:
		Due to JITF thirty (30) days prior to pre-test
		Due to JITF fourteen (14) days prior to pre-test
		Seven (7) days prior to pre-test

UNCLASSIFIED

Joint Test Readiness Review (JTRR) Clearances IPAT Package Software Delivery Self-assessment		Five (5) to ten (10) days prior to Beta I testing. Provide Date Time Group (DTG) prior to JTRR Provide at JTRR Provide at JTRR Provide at JTRR
Training Material Due		Start of Beta I testing.
Beta I Testing		Generally two (2) weeks total. See breakdown below.
JITF Testing		Generally five (5) days.
Security Testing		Generally three (3) days.
JITC Testing		Generally two (2) days.
JITC Final Interop Test Plan		Due to PMO fourteen (14) days following Beta I testing
JITF Draft Test Report		Delivered in softcopy five (5) days after completion of analyses.
Security Beta I Test Letter & Report (C&A Guide Appendices K & G)		Due five (5) days following Beta I NOTE: This is neither an IATO nor an IATT.
JITC Proceed to Beta II Test Letter		Due five (5) days following Beta I testing.
JITF Final Test Report		Delivered three (3) days after receipt of PMO comments on draft report.
Beta II Test		Date and Location. Scheduled no sooner than fifteen (15) days after completion of Beta I testing.
Beta II Site Test Message		Due twenty-one (21) days following Beta II testing.
Security Beta II Test Letter & Report (C&A Guide Appendices K & G)		Due twenty-one (21) days following Beta II testing. NOTE: This is neither an IATO nor an IATT.
JITC Interop Test Report		Due twenty-one (21) days following Beta II testing.
JITC Interop Certification Letter		Due twenty-eight (28) days following Beta II testing.
Training Certification Letter Issued		By Beta II test completion.

Docs = Documents Interop = Interoperability

****Note** “Days” are Calendar days**

UNCLASSIFIED

Unclassified

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 postponed or cancelled until documentation can be produced. The DExA for T&E shall coordinate with the testing components 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 Developmental Test and Evaluation (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 AFRL Security Office, Rome NY. (If the Beta I is conducted there.)
- 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 RECOMMENDED RESOURCE LIST

G.1.1 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.1.2 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 Local Area Network (LAN).

G.1.3 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.1.4 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 copier and facsimile capabilities.
- 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).

Unclassified

- g. If possible, test team should be able to work in the same test space during visit.

SECTION G.2 BETA II SITE CONFIRMATION LETTER MEMORANDUM

Date

MEMORANDUM FOR AFC2ISRC/INYE**

FROM: DoDIIS Beta II SITE
DoDIIS Beta II SITE POC

SUBJECT: DoDIIS Beta II SITE CONFIRMATION

1. (Unit) at (location) has agreed to be the DoDIIS Beta II test site for (system version xx) due to be tested on (date).
2. The critical interfaces required for complete DoDIIS Beta II testing of (system version xx) is/are
 - a. (interface 1)
 - b. (interface 2)
 - c. (interface 3...)

All critical interfaces listed are available at the site stated in paragraph 1. Sufficient space is also available for required testing.

3. Personnel from (unit) at (location) have agreed to be operators/users of (system) for Beta II testing purposes. (If the personnel are not from the Beta II site, a separate memorandum from their unit, stating those personnel will participate in the Beta II testing at (unit2) (location2), containing POC information for (unit2), and signed by their unit commander, must accompany this memorandum.)
4. The Beta II site POC for (unit) at (location) is (POC rank, name, commercial phone, DSN phone).

(Unit Commander Signature*)

(Unit commander signature block)

*Note 1: Unit Commander Signature cannot be electronic. A signed copy of this memorandum must be fax'd to Commercial (757) 225-0047 or DSN 575-0047 or scanned and e-mailed to dexa.te@langley.af.mil.

**Note 2: *This memo must be received by the DoDIIS DExA (Defense Executive Agent) for T&E (Testing and Evaluation) NLT 30 days prior to the start of DoDIIS Beta I testing.*

Unclassified

SECTION G.3 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:

Report Date: month dd yyyy

Program Name VERSION x.x BETA II TEST REPORT Tested on Month dd yyyy

[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, IACs and JITC, if applicable. This report will be sent out via AUTODIN, DMS or the existing official messaging system. To include the VTF at AFRL for posting.]

1. INTRODUCTION.

1.1 BACKGROUND. The *site name* has been directed by the Department of Defense Intelligence Information Systems (DoDIIS) Defense Management Board (DMB) to conduct Beta II testing for the *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.

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 /nonaccredited system. *[Or use some similar statements.] [This section will state the Beta II site's recommendation for fielding the specific program.]*

3. 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.

Unclassified

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 yy. 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 yy. 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.]

6. PROBLEM REPORTS

[Will list all generated during the Beta II test with comments.]

7. CHANGE REQUESTS

[Will list all generated during the Beta II test with comments.]

8. DOCUMENT REVIEW REPORTS

[Will list all generated during the Beta II test with comments.]

Unclassified

APPENDIX H - BETA I AND BETA II PMO SECURITY CERTIFICATION LETTER

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
(Information Assurance (IA)) Program."
b. DCID 6/3, "Security Policy for Uniform
Protection of Intelligence Processed in
Automated Information Systems and Networks."
c. DoDIIS Certification and Accreditation
Guide for Automated Information Systems (AIS)
Security in Intelligence Information Systems.
d. Joint DoDIIS/Cryptologic SCI Information
Systems Security Standards, April 2003
e. DCID 6/3 "Security Intelligence
Information Systems Processing National
Intelligence Information"

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.

Unclassified

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 Information Assurance (IA) 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
DEXA Test & Evaluation (DEXA for T&E)AFC2ISRC/INYE
VTF at AFRL

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 *DoDIIS Instructions*, outlines the procedures for acquiring DMB approval to field a software release to a DoDIIS site. PMOs will identify 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.

1.1 Version Release Identification. The following policy applies to initial and follow-on releases of an application. Software baselines and releases will be identified with a designator comprised of an integer to provide sequential numbering and decimal numbers indicating revision or version level. The first operational baseline version of the software will be identified with the designator 1.0. Releases of DoDIIS IMAs are to be categorized as major, minor or maintenance, with the PMO being responsible for assigning the version release number.

- Major releases are identified as ‘n.0’ (e.g. 1.0) and indicate a significant change in the architecture or operation of the application. A “rough rule of thumb” for PMOs to use for a significant change is 30 percent of the baseline changes.
- Minor releases are identified as ‘n.n’ (e.g. 1.1) in which new features are added to the application, but the fundamental architecture remains unchanged.
- Maintenance releases are identified as ‘n.n.n’ (e.g. 1.1.1) in which new features may be added to the application, but the emphasis is on optimization, feature enhancements, or modifications to improve stability and usability.
- Patches to applications correct a limited number of software problems reports and are identified as ‘n.n.n.n’ (e.g. 1.1.1.1).