CHANGE REQUEST COVER SHEET

Change Request Number: 09-94 **Date Received:** 12/1/2009

Title: Changes to IOT&E Sections of T&E Guidance Document

Name: David Woodson

Phone: 202-267-7601

Policy OR Guidance: Guidance

Section/Text Location Affected: Sections: 3.2.6, 5.3, Appendix C-11 and Appendix D of the T&E Guidance Document.

Summary of Change: Changes made to reflect organization name change from Office of IOT&E to Safety Assurance, and incorporation the SMS Risk Assessment Process which replaced the old IOT&E Issue. Per the AEB changed names of the acquisition documents.

Reason for Change: Changes in organizational structure and implementation of the SMS. Consistency of hazard rating between Service Teams and IOT&E are required.

Development, Review, and/or Concurrence: All of Safety Assurance has reviewed & approved along with SMS Director. Change to SMS Hazard Analysis has been briefed to all operational services.

Target Audience: Service Units with systems designated for IOT&E

Potential Links within FAST for the Change: None

Briefing Planned: Yes

ASAG Responsibilities: Review and Comment

Potential Links within FAST for the Change: None

Links for New/Modified Forms (or) Documents (LINK 1)

Links for New/Modified Forms (or) Documents (LINK 2)

Links for New/Modified Forms (or) Documents (LINK 3)

SECTIONS EDITED:

Test and Evaluation Process Guidelines:
Section 3.2.6 : Independent Operational Test and Evaluation [Old Content][New Content] [RedLine Content]
Test and Evaluation Process Guidelines:
Section 5.3 : OFFICE OF INDEPENDENT OPERATIONAL TEST AND EVALUATION [Old Content][New Content] [RedLine Content]
Test and Evaluation Process Guidelines:
C-11: SAMPLE IOTRD FORMAT [Old Content][New Content] [RedLine Content]
Test and Evaluation Process Guidelines:
D.1 IOT&E Documentation [Old Content][New Content] [RedLine Content]
Test and Evaluation Process Guidelines:
D2 IOT&E Team [Old Content][New Content] [RedLine Content]
Test and Evaluation Process Guidelines:
D.3 Relationship with Service Organizations [Old Content][New Content] [RedLine Content]
Test and Evaluation Process Guidelines:
D.4 IOT&E Designation Process [Old Content][New Content] [RedLine Content]
Test and Evaluation Process Guidelines:
D.5 IOT&E Method of System Assessment [Old Content][New Content] [RedLine Content]

SECTIONS EDITED:

Section 3.2.6 : Independent Operational Test and Evaluation

Old Content: Test and Evaluation Process Guidelines:
Section 3.2.6 : Independent Operational Test and Evaluation

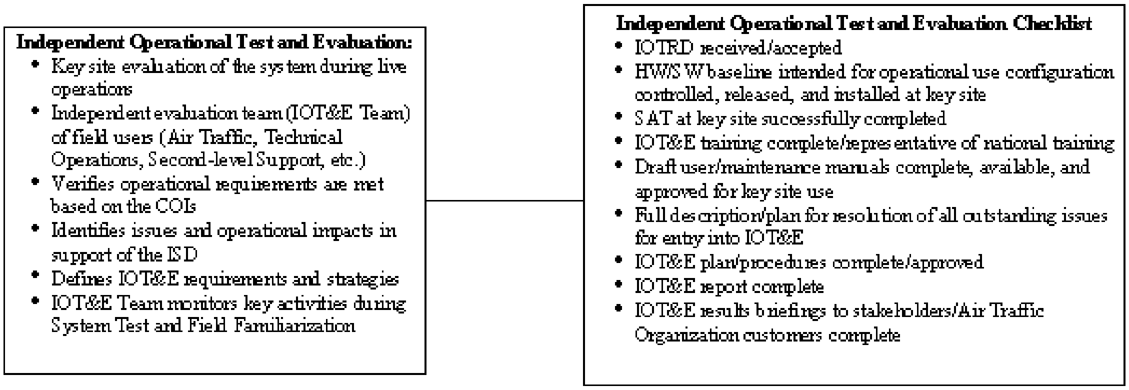
Figure 3.2-8 identifies associated processes and criteria for IOT&E activities within the SI or ISM phase of AMS. The processes and checklist criteria can be used to plan high-level T&E activities and to define initial entry and exit criteria. IOT&E is a full system-level evaluation conducted in an operational environment to confirm the operational readiness of a system to be part of the NAS. Therefore, IOT&E is performed on systems that have achieved initial operating capability (IOC) at an operational field facility (the key site). Data collection for IOT&E may begin prior to IOC if there are concerns about:

- HW/SW installation
- Transition between the system under evaluation and any legacy systems

Data collected prior to IOC supplements formal data collection during IOT&E. After IOC, the system undergoing IOT&E is an operational component of the NAS and must be operated and maintained by its intended users as designed for actual NAS operations. The results of IOT&E are used to support the ISD or other decisions regarding the operational use and deployment of systems.

The COO, through the Vice President of Safety Services, designates programs for IOT&E. Factors considered in designating programs include complexity, operational criticality, lifecycle cost, interoperability, and risk. An IOT&E is conducted by an IOT&E team that includes members from Air Traffic and Technical Operations and is led by a program manager from the Office of IOT&E. The strategy, resources, and schedule for IOT&E are documented in the T&E section of Exhibit 300 Program Baseline, Attachment 3: Implementation Strategy and Planning. The Office of IOT&E co-approves the T&E Section of the ISP for designated programs.

After formation, IOT&E teams are involved in monitoring key test events conducted earlier in SI or ISM to identify areas of operational risk. Identified risks are communicated to the service organization and may affect the scope of IOT&E. At the conclusion of system test activities, the Vice President of the implementing service organization declares the system ready for IOT&E via delivery of the IOTRD to the Vice President of Safety Services. Upon receipt of the IOTRD, and at the discretion of the Vice President of Safety Services, the IOT&E team commences IOT&E at the key site(s). At the conclusion of the IOT&E, the IOT&E team makes a determination of the system's operational readiness based on the operational risk associated with any identified issues. IOT&E results are briefed to the key site managers, the service organization, and Air Traffic Organization stakeholders at the Directorate and Vice President levels.



Independent Operational Test and Evaluation:

- Key site evaluation of the system during live operations
- Independent evaluation team (IOT&E Team) of field users (Air Traffic, Technical Operations, Second-level Support, etc.)
- Verifies operational requirements are met based on the COIs
- Identifies issues and operational impacts in support of the ISD
- Defines IOT&E requirements and strategies
- IOT&E Team monitors key activities during System Test and Field Familiarization

Independent Operational Test and Evaluation Checklist

- IOTRD received/accepted
- HW/SW baseline intended for operational use configuration controlled, released, and installed at key site
- SAT at key site successfully completed
- IOT&E training complete/representative of national training
- Draft user/maintenance manuals complete, available, and approved for key site use
- Full description/plan for resolution of all outstanding issues for entry into IOT&E
- IOT&E plan/procedures complete/approved
- IOT&E report complete
- IOT&E results briefings to stakeholders/Air Traffic Organization customers complete

Figure 3.2-8: IOT&E Checklist

New Content: Test and Evaluation Process Guidelines:
Section 3.2.6 : Independent Operational Test and Evaluation

Figure 3.2-8 identifies associated processes and criteria for IOT&E activities within the SI or ISM phase of AMS. The processes and checklist criteria can be used to plan high-level T&E activities and to define initial entry and exit criteria. IOT&E is a system-level evaluation conducted in an operational environment to confirm the operational readiness and identify the safety hazards of a system to be part of the NAS. Therefore, IOT&E is performed on systems that have achieved initial operating capability (IOC) at an operational field facility (the key site). Data collection at the key site for IOT&E may begin prior to IOC if there are concerns about:

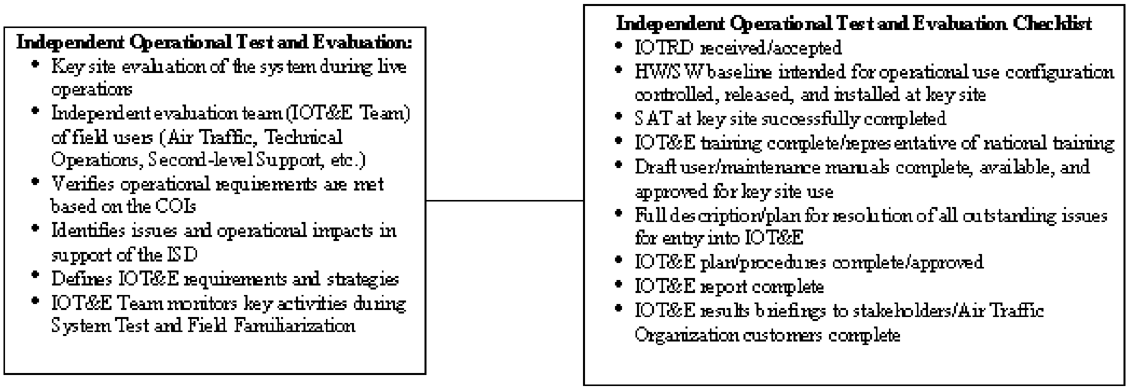
- HW/SW installation
- Transition between the system under evaluation and any legacy systems

Data collected from monitoring System Test prior to IOC supplements formal data collection during IOT&E. After IOC, the system undergoing IOT&E is an operational component of the NAS and must be operated and maintained by its intended users as designed for actual NAS operations. The results of IOT&E are used to support the ISD or other decisions regarding the operational use and deployment of systems.

The Vice President of Safety Services designates programs for IOT&E. Factors considered in designating programs include complexity, operational criticality, lifecycle cost, interoperability, and hazards. An IOT&E is conducted by an IOT&E team that includes members from Air Traffic, Technical Operations, and other system users and is led by a program manager from the Office of Safety Assurance. The strategy, resources, and schedule for IOT&E are documented in the T&E section of the Implementation Strategy and Planning Document (ISPD). The Office of Safety Assurance co-approves the T&E Section of the ISPD for designated programs.

After formation, IOT&E teams are involved in monitoring key test events conducted earlier in SI or ISM to identify operational hazards. Identified hazards are communicated to the service organization and may affect the scope of IOT&E. At the conclusion of System Test activities, the Vice President of the Service Unit declares to the Vice President of the Office of Safety via IOTRD the system's readiness for IOT&E and operational use. Upon receipt of the IOTRD, and at the discretion of the Vice President of Safety Services, the IOT&E team commences IOT&E at the key site(s). At the conclusion of the IOT&E, the IOT&E team makes a determination of the system's operational readiness based on the safety hazards associated with any identified issues. IOT&E results are briefed to the key site managers, the service organization, and Air Traffic Organization stakeholders at the Directorate and Vice President levels.

- Independent Operational Test and Evaluation Characteristics:
- Key site evaluation of the system during live operations
- Independent evaluation team (IOT&E Team) of field users (Air Traffic, Technical Operations, Second-level Support, etc.)
- Verification of the meeting of operational requirements based on the COIs
- Identification of hazards and the operational readiness of the system in support of the ISD
- Definition of IOT&E requirements and strategies
- Monitoring by the IOT&E Team of key activities during System Test and Field



Independent Operational Test and Evaluation:

- Key site evaluation of the system during live operations
- Independent evaluation team (IOT&E Team) of field users (Air Traffic, Technical Operations, Second-level Support, etc.)
- Verifies operational requirements are met based on the COIs
- Identifies issues and operational impacts in support of the ISD
- Defines IOT&E requirements and strategies
- IOT&E Team monitors key activities during System Test and Field Familiarization

Independent Operational Test and Evaluation Checklist

- IOTRD received/accepted
- HW/SW baseline intended for operational use configuration controlled, released, and installed at key site
- SAT at key site successfully completed
- IOT&E training complete/representative of national training
- Draft user/maintenance manuals complete, available, and approved for key site use
- Full description/plan for resolution of all outstanding issues for entry into IOT&E
- IOT&E plan/procedures complete/approved
- IOT&E report complete
- IOT&E results briefings to stakeholders/Air Traffic Organization customers complete

Figure 3.2-8: IOT&E Checklist

Red Line Content: Test and Evaluation Process Guidelines:
Section 3.2.6 : Independent Operational Test and Evaluation

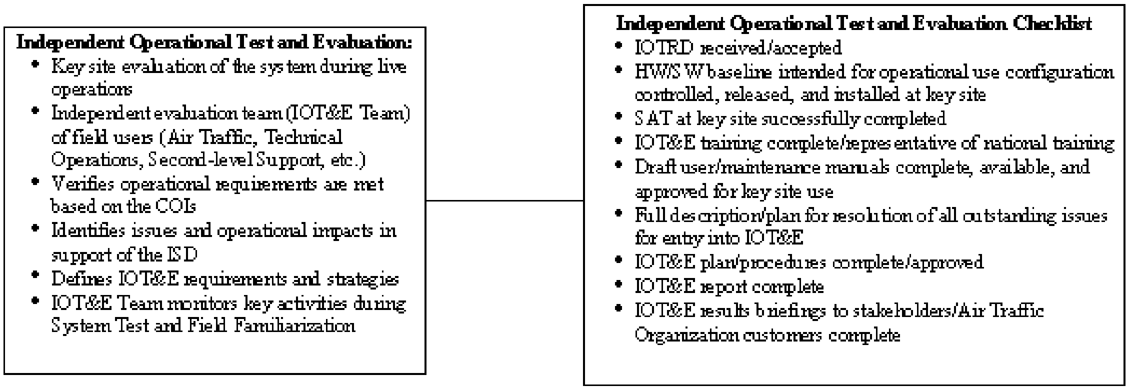
Figure 3.2-8 identifies associated processes and criteria for IOT&E activities within the SI or ISM phase of AMS. The processes and checklist criteria can be used to plan high-level T&E activities and to define initial entry and exit criteria. IOT&E is a ~~full~~ system-level evaluation conducted in an operational environment to confirm the operational readiness ***and identify the safety hazards*** of a system to be part of the NAS. Therefore, IOT&E is performed on systems that have achieved initial operating capability (IOC) at an operational field facility (the key site). Data collection ***at the key site*** for IOT&E may begin prior to IOC if there are concerns about:

- HW/SW installation
- Transition between the system under evaluation and any legacy systems

Data collected ***from monitoring System Test*** prior to IOC supplements formal data collection during IOT&E. After IOC, the system undergoing IOT&E is an operational component of the NAS and must be operated and maintained by its intended users as designed for actual NAS operations. The results of IOT&E are used to support the ISD or other decisions regarding the operational use and deployment of systems. ~~The COO, through the~~
The Vice President of Safety Services~~,~~ designates programs for IOT&E. Factors considered in designating programs include complexity, operational criticality, lifecycle cost, interoperability, and ~~risk~~***hazards***. An IOT&E is conducted by an IOT&E team that includes members from Air Traffic~~ and~~***,*** Technical Operations***, and other system users*** and is led by a program manager from the Office of ~~IOT&E~~***Safety Assurance***. The strategy, resources, and schedule for IOT&E are documented in the T&E section of ~~Exhibit 300 Program Baseline, Attachment 3:~~***the*** Implementation Strategy and Planning ***Document (ISPD)***. The Office of ~~IOT&E~~***Safety Assurance*** co-approves the T&E Section of the ~~ISP~~***ISPD*** for designated programs. ~~After~~

After formation, IOT&E teams are involved in monitoring key test events conducted earlier in SI or ISM to identify ~~areas of~~ operational ~~risk~~***hazards***. Identified ~~risks~~***hazards*** are communicated to the service organization and may affect the scope of IOT&E. At the conclusion of ~~system test~~***System Test*** activities, the Vice President of the ~~implementing~~***Service*** ~~service organization~~***Unit*** declares ~~the system ready for~~***to the Vice President*** ~~IOT&E~~***of*** ~~via delivery~~***the Office*** of ~~the~~***Safety*** ~~IOTRD to~~***via IOTRD*** the ~~Vice~~***system's*** ~~President of~~***readiness for*** ~~Safety~~***IOT&E*** ~~Services~~***and operational use***. Upon receipt of the IOTRD, and at the discretion of the Vice President of Safety Services, the IOT&E team commences IOT&E at the key site(s). At the conclusion of the IOT&E, the IOT&E team makes a determination of the system's operational readiness based on the ~~operational risk~~***safety hazards*** associated with any identified issues. IOT&E results are briefed to the key site managers, the service organization, and Air Traffic Organization stakeholders at the Directorate and Vice President levels.

- ***Independent Operational Test and Evaluation Characteristics:***
- ***Key site evaluation of the system during live operations***
- ***Independent evaluation team (IOT&E Team) of field users (Air Traffic, Technical Operations, Second-level Support, etc.)***
- ***Verification of the meeting of operational requirements based on the COIs***
- ***Identification of hazards and the operational readiness of the system in support of the ISD***
- ***Definition of IOT&E requirements and strategies***
- ***Monitoring by the IOT&E Team of key activities during System Test and Field***



Independent Operational Test and Evaluation:
- Key site evaluation of the system during live operations
- Independent evaluation team (IOT&E Team) of field users (Air Traffic, Technical Operations, Second-level Support, etc.)
- Verifies operational requirements are met based on the COIs
- Identifies issues and operational impacts in support of the ISD
- Defines IOT&E requirements and strategies
- IOT&E Team monitors key activities during System Test and Field Familiarization

Independent Operational Test and Evaluation Checklist
- IOTRD received/accepted
- HW/SW baseline intended for operational use configuration controlled, released, and installed at key site
- SAT at key site successfully completed
- IOT&E training complete/representative of national training
- Draft user/maintenance manuals complete, available, and approved for key site use
- Full description/plan for resolution of all outstanding issues for entry into IOT&E
- IOT&E plan/procedures complete/approved
- IOT&E report complete
- IOT&E results briefings to stakeholders/Air Traffic Organization customers complete

Figure 3.2-8: IOT&E Checklist

Section 5.3 : OFFICE OF INDEPENDENT OPERATIONAL TEST AND EVALUATION

Old Content: Test and Evaluation Process Guidelines:
Section 5.3 : OFFICE OF INDEPENDENT OPERATIONAL TEST AND EVALUATION

The Office of IOT&E is responsible for planning and conducting IOT&E on designated programs. The Office of IOT&E develops IOT&E sections for inclusion in the T&E section of Exhibit 300 Program Baseline, Attachment 3: Implementation Strategy and Planning. The Office of IOT&E co-approves the ISP T&E section on programs designated for IOT&E. The IOT&E team develops IOT&E plans and procedures. The Office of IOT&E also provides assistance in the development of COIs for inclusion in the program's Exhibit 300 Program Baseline, Attachment 1: Program Requirements.

New Content: Test and Evaluation Process Guidelines:
Section 5.3 : OFFICE OF INDEPENDENT OPERATIONAL TEST AND EVALUATION

The Office of Safety Assurance is responsible for planning and conducting IOT&E on designated programs. It develops IOT&E sections for inclusion in the T&E section of the Implementation Strategy and Planning Document (ISPD) and co-approves the ISPD T&E section on programs designated for IOT&E. The IOT&E team develops IOT&E plans and procedures. The Office of Safety Assurance also provides assistance in the development of COIs for inclusion in the program's Program Requirements Document.

Red Line Content: Test and Evaluation Process Guidelines:
Section 5.3 : OFFICE OF INDEPENDENT OPERATIONAL TEST AND EVALUATION

The Office of ~~IOT&E~~***Safety Assurance*** is responsible for planning and conducting IOT&E on designated programs.~~ The Office of IOT&E~~***It*** develops IOT&E sections for inclusion in the T&E section of ~~Exhibit 300 Program Baseline, Attachment 3:~~***the*** Implementation Strategy and Planning~~. The Office~~***Document*** ~~of~~***(ISPD)*** ~~IOT&E~~***and*** co-approves the ~~ISP~~***ISPD*** T&E section on programs designated for IOT&E. The IOT&E team develops IOT&E plans and procedures. The Office of ~~IOT&E~~***Safety Assurance*** also provides assistance in the development of COIs for inclusion in the program's ~~Exhibit 300 Program Baseline, Attachment 1:~~ Program Requirements ***Document***.

C-11: SAMPLE IOTRD FORMAT

Old Content: Test and Evaluation Process Guidelines:
C-11: SAMPLE IOTRD FORMAT

Appendix C-11

[Sample IOTRD Format]

[6/10/08]

[Note: The IOTRD should provide details about the **current** status of the system. It **does not** describe what will be done to the system **in the future**, but rather what state it is in **at this point**.]

1.0 Test Status

1.1 Status

[Report the status of DT and OT. It is expected that DT and OT have been successfully completed and have met all exit criteria. State whether the AMS T&E Guidance was followed or tailored. If it was tailored, describe what was changed. State whether the T&E Gold Standard was used.]

1.2 Results

[Summarize the **results** of DT and OT. The write-up should detail which tests/requirements, if any, have failed. Typically, the summary states that tests indicate the system will be ready for approval at the In-Service Decision milestone. For open items from OT and DT, the IOTRD should contain an appendix that provides the disposition of each (e.g., deferred to next phase," "planned for closure prior to IOT&E," "fix planned for Build XXX").]

1.3 Test Report and Distribution

[Summarize the test report and distribution status. A representative entry might state that DT reports and Quick-Look OT reports have been completed and distributed to the appropriate parties, including the Office of SSIA and all test participants. Include information about any supplemental test reports that provide additional information on DT or OT results.]

2.0 System Status

2.1 Open PTRs

[Summarize the number of open PTRs and their significance (type) and overall impact on system performance, suitability, and effectiveness. Identify any PTRs that will **not** be closed before the start of IOT&E, along with expected closure date. Identify any limitations to operational use that the open PTRs might pose.]

2.2 System Stability

[Describe the stability of the system in terms of configuration management and baselining. Include a list of all unapproved or pending deviations/waivers. For example, "system hardware, software, and specifications are baselined and under the configuration control of the NAS CCB." The IOTRD should address the **national baseline** of the system. Describe the schedule for any planned software or hardware revisions required during IOT&E and how they will be handled. If the system is not under NAS CCB control, a description of the configuration management process should be included.]

2.3 Status of Hazards from the Pre-IOT&E Hazard Paper

[Provide a table or appendix that contains the current status of the hazards documented in the Pre-IOT&E Hazard Paper.]

Hazard	**Current Status [(Current Date)]**
[Hazard Statement]	[status]
[Hazard Statement]	[status]
[Hazard Statement]	[status]

3.0 IOT&E Prerequisite Status

[Provide the status of each IOT&E prerequisite detailed in the T&E section of the program's ISP (Attachment 3 of Exhibit 300) and the proposed workaround if the prerequisite is not ready/available/complete.]

3.1 Status of Site Acceptance

[Provide the status of Site Acceptance by the FAA at the key site.]

3.2 Equipment Support Status

[Describe the support equipment for the system. A typical statement might be: "Spares for all FAA-maintained equipment are on site, and the logistics center will maintain a two year supply of spares for the LRU. Leased equipment will be maintained by the __________Company."]

3.3 Technical Operations Manuals

[Describe the status of Technical Operations manuals. Are they available, verified, and approved for use at the key site?]

3.4 Training Status

[Describe the training given to operational facility personnel. For example, "Personnel who will operate and maintain the system during IOT&E have received the approved training, which is representative of the training that will be given to operational personnel at downstream sites."]

3.5 AT Procedures Status

[If changes are/were required to AT procedures, state whether the new procedures have been approved or incorporated into the appropriate documentation (i.e., FAA Order 7110.65).]

3.6 Safety Status

[The current signed SRMD, updated with the results from OT, should be provided or discuss the areas the Service Team has updated.]

3.7 Readiness for Operational Use

[Describe any concerns (e.g., training, procedures, system stability) with using the system operationally at the key site.]

3.8 IOC

[Describe the readiness of the site to declare IOC.]

3.9 Additional Sites

[Describe any additional sites that will declare IOC or have already declared IOC prior to the ISD, which is not permitted by the AMS.]

4.0 Exceptions

[Identify and describe any outstanding exceptions to the readiness of the system for operational use at key site (see sections 1.0 through 3.0, above). Describe the **operational impact** of the exception(s) and the **justification** for proceeding with an IOTRD despite the exception(s). An exception is considered an open/unresolved item or deficiency that has a **potential significant operational impact**. These problems usually impact system performance or require an operational workaround by the users.]

5.0 Recommendation

[Clearly state the recommendation and any associated conditions. For example, "The system is ready for operational use. [Responsible Service Organization] recommends proceeding before the PTRs identified in section 2.1 are closed.")]

Declaration of Readiness: Signed, [VP of the Responsible Service Organization]

New Content: Test and Evaluation Process Guidelines:
C-11: SAMPLE IOTRD FORMAT

Appendix C-11

[Sample IOTRD Format]

[Note: The IOTRD should provide details about the **current** status of the system. It **does not** describe what will be done to the system **in the future**, but rather what state it is in **at this point**.]

1.0 Test Status

1.1 Status

[Report the status of DT and OT. It is expected that DT and OT have been successfully completed and have met all exit criteria. State whether the AMS T&E Guidance was followed or tailored. If it was tailored, describe what was changed. State whether the T&E Gold Standard was used.]

1.2 Results

[Summarize the **results** of DT and OT. The write-up should detail which tests/requirements, if any, have failed. Typically, the summary states that tests indicate the system will be ready for approval at the In-Service Decision milestone. For open items from OT and DT, the IOTRD should contain an appendix that provides the disposition of each (e.g., deferred to next phase," "planned for closure prior to IOT&E," "fix planned for Build XXX").]

1.3 Test Report and Distribution

[Summarize the test report and distribution status. A representative entry might state that DT reports and Quick-Look OT reports have been completed and distributed to the appropriate parties, including the Office of SSIA and all test participants. Include information about any supplemental test reports that provide additional information on DT or OT results.]

2.0 System Status

2.1 Open PTRs

[Summarize the number of open PTRs and their significance (type) and overall impact on system performance, suitability, and effectiveness. Identify any PTRs that will **not** be closed before the start of IOT&E, along with expected closure date. Identify any limitations to operational use that the open PTRs might pose.]

2.2 System Stability

[Describe the stability of the system in terms of configuration management and baselining. Include a list of all unapproved or pending deviations/waivers. For example, "system hardware, software, and specifications are baselined and under the configuration control of the NAS CCB." The IOTRD should address the **national baseline** of the system. Describe the schedule for any planned software or hardware revisions required during IOT&E and how they will be handled. If the system is not under NAS CCB control, a description of the configuration management process should be included.]

2.3 Status of Hazards from the Pre-IOT&E Paper

[Provide a table or appendix that contains the current status of the hazards documented in the Pre-IOT&E Paper.]

Hazard	**Current Status [(Current Date)]**
[Hazard Statement]	[status]
[Hazard Statement]	[status]
[Hazard Statement]	[status]

3.0 IOT&E Prerequisite Status

[Provide the status of each IOT&E prerequisite detailed in the T&E section of the program's Implementation Strategy and Planning Document (ISPD) and the proposed workaround if the prerequisite is not ready/available/complete.]

3.1 Status of Site Acceptance

[Provide the status of Site Acceptance by the FAA at the key site.]

3.2 Equipment Support Status

[Describe the support equipment for the system. A typical statement might be: "Spares for all FAA-maintained equipment are on site, and the logistics center will maintain a two year supply of spares for the LRU. Leased equipment will be maintained by the __________Company."]

3.3 Technical Operations Manuals

[Describe the status of Technical Operations manuals. Are they available, verified, and approved for use at the key site?]

3.4 Training Status

[Describe the training given to operational facility personnel. For example, "Personnel who will operate and maintain the system during IOT&E have received the approved training, which is representative of the training that will be given to operational personnel at downstream sites."]

3.5 AT Procedures Status

[If changes are/were required to AT procedures, state whether the new procedures have been approved or incorporated into the appropriate documentation (i.e., FAA Order 7110.65).]

3.6 Safety Status

[The current signed SRMD, updated with the results from OT, should be provided. Provide the current status of each hazard, and associated mitigations, identified in the most current SRMD, as reflected in the monitoring plan.]

3.7 Readiness for Operational Use

[Describe any concerns (e.g., training, procedures, system stability) with using the system operationally at the key site.]

3.8 IOC

[Describe the readiness of the site to declare IOC.]

3.9 Additional Sites

[Describe any additional sites that will declare IOC or have already declared IOC prior to the ISD, which is not permitted by the AMS.]

4.0 Exceptions

[Identify and describe any outstanding exceptions to the readiness of the system for operational use at key site (see sections 1.0 through 3.0, above). Describe the **operational impact** of the exception(s) and the **justification** for proceeding with an IOTRD despite the exception(s). An exception is considered an open/unresolved item or deficiency that has a **potential significant operational impact**. These problems usually impact system performance or require an operational workaround by the users.]

5.0 Recommendation

[Clearly state the recommendation and any associated conditions. For example, "The system is ready for operational use. [Responsible Service Organization] recommends proceeding before the PTRs identified in section 2.1 are closed.")]

Declaration of Readiness: Signed, [VP of the Responsible Service Organization] [Date}

Red Line Content: Test and Evaluation Process Guidelines:
C-11: SAMPLE IOTRD FORMAT

[Sample IOTRD Format]

[~~6~~***3***/~~10~~***22***/~~08~~***10***]

[Note: The IOTRD should provide details about the **current** status of the system. It **does not** describe what will be done to the system **in the future**, but rather what state it is in **at this point**.]

1.0 Test Status

1.1 Status

[Report the status of DT and OT. It is expected that DT and OT have been successfully completed and have met all exit criteria. State whether the AMS T&E Guidance was followed or tailored. If it was tailored, describe what was changed. State whether the T&E Gold Standard was used.]

1.2 Results

[Summarize the **results** of DT and OT. The write-up should detail which tests/requirements, if any, have failed. Typically, the summary states that tests indicate the system will be ready for approval at the In-Service Decision milestone. For open items from OT and DT, the IOTRD should contain an appendix that provides the disposition of each (e.g., deferred to next phase," "planned for closure prior to IOT&E," "fix planned for Build XXX").]

1.3 Test Report and Distribution

[Summarize the test report and distribution status. A representative entry might state that DT reports and Quick-Look OT reports have been completed and distributed to the appropriate parties, including the Office of SSIA and all test participants. Include information about any supplemental test reports that provide additional information on DT or OT results.]

2.0 System Status

2.1 Open PTRs

[Summarize the number of open PTRs and their significance (type) and overall impact on system performance, suitability, and effectiveness. Identify any PTRs that will **not** be closed before the start of IOT&E, along with expected closure date. Identify any limitations to operational use that the open PTRs might pose.]

2.2 System Stability

[Describe the stability of the system in terms of configuration management and baselining. Include a list of all unapproved or pending deviations/waivers. For example, "system hardware, software, and specifications are baselined and under the configuration control of the NAS CCB." The IOTRD should address the **national baseline** of the system. Describe the schedule for any planned software or hardware revisions required during IOT&E and how they will be handled. If the system is not under NAS CCB control, a description of the configuration management process should be included.]

2.3 Status of Hazards from the Pre-IOT&E ~~Hazard~~ Paper

[Provide a table or appendix that contains the current status of the hazards documented in the Pre-IOT&E ~~Hazard~~ Paper.]

Hazard	**Current Status [(Current Date)]**
[Hazard Statement]	[status]
[Hazard Statement]	[status]
[Hazard Statement]	[status]

3.0 IOT&E Prerequisite Status

[Provide the status of each IOT&E prerequisite detailed in the T&E section of the program's ~~ISP~~***Implementation*** ~~(Attachment~~***Strategy*** ~~3 of Exhibit~~***and Planning Document*** ~~300~~***(ISPD***) and the proposed workaround if the prerequisite is not ready/available/complete.]

3.1 Status of Site Acceptance

[Provide the status of Site Acceptance by the FAA at the key site.]

3.2 Equipment Support Status

[Describe the support equipment for the system. A typical statement might be: "Spares for all FAA-maintained equipment are on site, and the logistics center will maintain a two year supply of spares for the LRU. Leased equipment will be maintained by the __________Company."]

3.3 Technical Operations Manuals

[Describe the status of Technical Operations manuals. Are they available, verified, and approved for use at the key site?]

3.4 Training Status

[Describe the training given to operational facility personnel. For example, "Personnel who will operate and maintain the system during IOT&E have received the approved training, which is representative of the training that will be given to operational personnel at downstream sites."]

3.5 AT Procedures Status

[If changes are/were required to AT procedures, state whether the new procedures have been approved or incorporated into the appropriate documentation (i.e., FAA Order 7110.65).]

3.6 Safety Status

[The current signed SRMD, updated with the results from OT, should be provided~~ or~~. ~~discuss~~***Provide*** the ~~areas~~***current status of each hazard, and associated mitigations, identified in*** the ~~Service~~***most current*** ~~Team~~***SRMD,*** ~~has~~***as*** ~~updated~~***reflected in the monitoring plan***.]

3.7 Readiness for Operational Use

[Describe any concerns (e.g., training, procedures, system stability) with using the system operationally at the key site.]

3.8 IOC

[Describe the readiness of the site to declare IOC.]

3.9 Additional Sites

[Describe any additional sites that will declare IOC or have already declared IOC prior to the ISD, which is not permitted by the AMS.]

4.0 Exceptions

[Identify and describe any outstanding exceptions to the readiness of the system for operational use at key site (see sections 1.0 through 3.0, above). Describe the **operational impact** of the exception(s) and the **justification** for proceeding with an IOTRD despite the exception(s). An exception is considered an open/unresolved item or deficiency that has a **potential significant operational impact**. These problems usually impact system performance or require an operational workaround by the users.]

5.0 Recommendation

[Clearly state the recommendation and any associated conditions. For example, "The system is ready for operational use. [Responsible Service Organization] recommends proceeding before the PTRs identified in section 2.1 are closed.")]

Declaration of Readiness: Signed, [VP of the Responsible Service Organization] ***[Date}***

D.1 IOT&E Documentation

Old Content: Test and Evaluation Process Guidelines:
D.1 IOT&E Documentation

During early program monitoring, the Office of IOT&E identifies risks and communicates these risks to the service organization via informal verbal communication and formal written communication. IOT&E required documentation includes input to the ISP test and evaluation section, an IOT&E plan, an IOT&E procedures document, and an IOT&E Team assessment report (IOT&E Report). Figure

D1-1 depicts a generic timeline of IOT&E activities and shows when supporting IOT&E documents would normally be developed.

IOT&E Input to the ISP T&E Sections. The Office of IOT&E reviews and comments on the service organization's T&E strategy proposed in the ISP. The Office of IOT&E also provides the IOT&E section for the ISP. For the ISP T&E section, The Office of IOT&E documents the IOT&E activities, resources, and strategy. The Office of IOT&E has full approval of the IOT&E section of the ISP.

Office of IOT&E Co-approval of T&E Section of ISP. The Office of IOT&E, along with the service team lead, co-approves the entire T&E section of the ISP. The Office of IOT&E prepares a signature page for the front of the ISP T&E section and a memo to the service team lead detailing any issues or conditions prior to co-approval.

IOT&E plans and procedures. The IOT&E plans and procedures documents should include scheduling, resources, coverage of system test, and data collection and analysis to allow a formal IOT&E team assessment of the system's operational readiness.

Pre-IOT&E Operational Issue Paper. Subsequent to OT completion and prior to the IOTRD, the Office of IOT&E and the IOT&E team prepare an issue paper for the ATO stakeholders and service organization that provides a summary of the operational issues that are being tracked as IOT&E approaches.

Reports. The IOT&E report will be distributed to the service organization and all ATO stakeholders at the Directorate and Vice President levels. The report will also be sent to the ATO COO. This report supports a production decision or in-service decision. Due to the independent nature of the IOT&E report, there is no formal comment/review process outside of the IOT&E team. The IOT&E report is based on all data available at that time.

Follow-on Assessment and Reporting. The Office of IOT&E, along with the IOT&E team, provides a follow-up assessment on any new operational issues identified after the ISD and a status of significant operational issues that were identified in the original IOT&E report. Results of the follow-up assessment are detailed in a follow-up report issued approximately six months following the ISD.

Figure D1-1: Generic Timeline of IOT&E Activities

Click here to view figure

New Content: Test and Evaluation Process Guidelines:
D.1 IOT&E Documentation

During early program monitoring, the Office of Safety Assurance identifies potential hazards and communicates them to the service organization via informal verbal communication and formal written communication. IOT&E required documentation includes input to the ISPD test and evaluation section, an IOT&E plan, an IOT&E procedures document, and an IOT&E Team assessment report (IOT&E Report). Figure D1-1 depicts a generic timeline of IOT&E activities and shows when supporting IOT&E documents would normally be developed.

IOT&E Input to the ISPD T&E Sections. The Office of Safety Assurance reviews and comments on the service organization's T&E strategy proposed in the ISPD. The Office of Safety Assurance also provides the IOT&E section for the ISPD. For the ISPD T&E section, The Office of Safety Assurance documents the IOT&E activities, resources, and strategy. The Office of Safety Assurance has full approval of the IOT&E section of the ISPD.

Office of Safety Assurance Co-approval of T&E Section of ISPD. The Office of Safety Assurance, along with the service team lead, co-approves the entire T&E section of the ISPD. The Office of Safety Assurance prepares a signature page for the front of the ISPD T&E section, and, if applicable, a memo to the service team lead detailing any issues or conditions prior to co-approval.

IOT&E plans and procedures. The IOT&E plans and procedures documents should include scheduling, resources, coverage of system test, and data collection and analysis to allow a formal IOT&E team assessment of the system's operational readiness.

Pre-IOT&E Status Paper. Subsequent to OT completion and prior to the IOTRD, the Office of Safety Assurance and the IOT&E team prepare a status paper for the service organization that provides a summary of the potential risks that are being tracked as IOT&E approaches.

Intermediate Email. Halfway through IOT&E (and during Data Reduction and Analysis (DR&A), if new significant concerns are identified), the PM sends an email summarizing, at a high level (i.e., not IIS data), significant concerns to the Service Team Lead (see Intermediate Email template).
Preliminary IOT&E Report. A Preliminary IOT&E Report may be developed to allow for the earlier identification and resolution of hazards prior to the ISD (see template). Once the program is designated for IOT&E, the PM must discuss this option with the

Service Team Lead. The PM should promote the benefits of a Preliminary IOT&E Report but stress its effect on the program schedule. The Service Team's decision on having a Preliminary IOT&E Report must be documented in an email from the PM to the Service Team Lead and the SA Manager, with a "cc:" to the Director. The decision can also be recorded in the ISPD if it has not been finalized. The Preliminary IOT&E Report is prepared during the IOT&E caucus and includes the identified hazards and ratings, an Executive Summary, and does not include an assessment of Operational Readiness.

The Service Team must respond to the Preliminary IOT&E Report via memorandum at a minimum of five weeks prior to the ISD, indicating that the system is ready to be assessed for Operational Readiness. The length of time for IOT&E activities after the Service Team's response may need to be negotiated if major changes are made to the system after the Preliminary IOT&E Report. Upon receiving the Service Team response, the IOT&E Team Lead reconvenes the team to re-evaluate the system. At this time, the system is assessed for Operational Readiness.
Report. The IOT&E report will be distributed to the service organization and all ATO stakeholders at the Directorate and Vice President levels. This report supports the in-service decision. Due to the independent nature of the IOT&E report, there is no formal comment/review process outside of the IOT&E team. The IOT&E report is based on all data available at that time.

Follow-on Assessment and Reporting. The Office of Safety Assurance, along with the IOT&E team, provides a follow-up assessment on any new hazards/risks identified after the ISD and a status of significant hazards that were identified in the original IOT&E report. Results of the follow-up assessment are detailed in a follow-up report issued approximately six months following the ISD.

Figure D1-1: Generic Timeline of IOT&E Activities

Click here to view figure

Red Line Content: Test and Evaluation Process Guidelines:
D.1 IOT&E Documentation

During early program monitoring, the Office of ~~IOT&E~~***Safety Assurance*** identifies ~~risks~~***potential hazards*** and communicates ~~these risks~~***them*** to the service organization via informal verbal communication and formal written communication. IOT&E required documentation includes input to the ~~ISP~~***ISPD*** test and evaluation section, an IOT&E plan, an IOT&E procedures document, and an IOT&E Team assessment report (IOT&E Report). Figure D1-1 depicts a generic timeline of IOT&E activities and shows when supporting IOT&E documents would normally be developed.

IOT&E Input to the ~~ISP~~*ISPD* T&E Sections. The Office of ~~IOT&E~~***Safety Assurance*** reviews and comments on the service organization's T&E strategy proposed in the

~~ISP~~ISPD. The Office of ~~IOT&E~~Safety Assurance also provides the IOT&E section for the ~~ISP~~ISPD. For the ~~ISP~~ISPD T&E section, The Office of ~~IOT&E~~Safety Assurance documents the IOT&E activities, resources, and strategy. The Office of ~~IOT&E~~Safety Assurance has full approval of the IOT&E section of the ~~ISP~~ISPD.

Office of ~~IOT~~&~~amp~~#160;~~E~~Safety Assurance Co-approval of T&E Section of ~~ISP~~ISPD. The Office of ~~IOT&E~~Safety Assurance, along with the service team lead, co-approves the entire T&E section of the ~~ISP~~ISPD. The Office of ~~IOT&E~~Safety Assurance prepares a signature page for the front of the ~~ISP~~ISPD T&E section, and, if applicable, a memo to the service team lead detailing any issues or conditions prior to co-approval.

IOT&E plans and procedures. The IOT&E plans and procedures documents should include scheduling, resources, coverage of system test, and data collection and analysis to allow a formal IOT&E team assessment of the system's operational readiness.

Pre-IOT&E ~~Operational Issue~~ Status Paper. Subsequent to OT completion and prior to the IOTRD, the Office of ~~IOT&E~~Safety Assurance and the IOT&E team prepare ~~an issue~~a status paper for the ~~ATO stakeholders and~~ service organization that provides a summary of the ~~operational issues~~potential risks that are being tracked as IOT&E approaches.

~~Reports~~Intermediate Email. ~~The~~Halfway through IOT&E ~~report~~(and ~~will~~during Data Reduction and Analysis (DR&A), if new significant concerns are identified), the PM sends an email summarizing, at a high level (i.e., not IIS data), significant concerns to the Service Team Lead (see Intermediate Email template).

Preliminary IOT&E Report. A Preliminary IOT&E Report may be ~~distributed~~developed to allow for the ~~service organization~~earlier identification and ~~all~~resolution ~~ATO stakeholders at~~of hazards prior to the ~~Directorate~~ISD (see template). Once the program is designated for IOT&E, the PM must discuss this option with the Service Team Lead. The PM should promote the benefits of a Preliminary IOT&E Report but stress its effect on the program schedule. The Service Team's decision on having a Preliminary IOT&E Report must be documented in an email from the PM to the Service Team Lead and ~~Vice President~~the SA ~~levels~~Manager, with a "cc:" to the Director. The ~~report will~~decision can also be ~~sent~~recorded ~~to~~in the ~~ATO~~ISPD if it has ~~COO~~not been finalized. ~~This report~~The ~~supports~~Preliminary IOT&E Report is prepared during the IOT&E caucus and includes the identified hazards and ratings, an Executive Summary, and does not include an assessment of Operational Readiness.

The Service Team must respond to the Preliminary IOT&E Report via memorandum at a ~~production decision or~~minimum of five ~~in~~weeks prior to the ISD, indicating that the system is ready to be assessed for Operational Readiness. The length of time for IOT&E activities after the Service Team's response may need to be negotiated if major changes are made to the system after the Preliminary IOT&E Report. Upon receiving the Service Team response, the IOT&E Team Lead reconvenes the team to re-evaluate the system. At this time, the system is assessed for Operational Readiness.

Report. The IOT&E report will be distributed to the service ~~decision~~***organization and all ATO stakeholders at the Directorate and Vice President levels***. ***This report supports the in-service decision.*** Due to the independent nature of the IOT&E report, there is no formal comment/review process outside of the IOT&E team.~~-~~ The IOT&E report is based on all data available at that time.

Follow-on Assessment and Reporting. The Office of ~~IOT&E~~***Safety Assurance***, along with the IOT&E team, provides a follow-up assessment on any new ~~operational issues~~***hazards/risks*** identified after the ISD and a status of significant ~~operational issues~~***hazards*** that were identified in the original IOT&E report.~~-~~ Results of the follow-up assessment are detailed in a follow-up report issued approximately six months following the ISD.

Figure D1-1: Generic Timeline of IOT&E Activities

Click here to view figure

D2 IOT&E Team

Old Content: Test and Evaluation Process Guidelines:

D2 IOT&E Team

Organizations that operate, maintain, or are otherwise operationally affected by the implementation of a new system are represented on the IOT&E team. IOT&E teams will include subject-matter experts at both the working level and supervisory levels from Headquarters and field operations.

The Office of IOT&E coordinates with appropriate ATO offices to obtain IOT&E team members from field facilities. Additional participants may include FAA personnel who are system users such as the National Weather Service, and the Department of Defense.

Office of IOT&E's Role in IOT&E. The IOT&E program manager from the Office of IOT&E leads and provides full administrative support to the IOT&E team during IOT&E. The Office of IOT&E facilitates the final IOT&E team system assessment by ensuring proper collection, analysis, and reporting of test results. The IOT&E team reports the operational assessment of the evaluated system to the in-service decision authority. The Director of the Office of IOT&E represents independent test and evaluation within the FAA.

IOT&E Team Responsibility. The IOT&E team is responsible for conducting independent operational assessments of designated programs. Although every attempt will be made to keep members' management informed of assessments and recommendations, IOT&E team assessments and/or recommendations will be based solely on the analyses of system performance and capabilities during IOT&E and of data collected during earlier test phases.

Role of IOT&E Team During System Test and Field Familiarization. IOT&E may use the results from selected SI system test events to aid the resolution of COIs. Members from the IOT&E team observe selected system test events and have access to all system test and PTR data so that a complete IOT&E assessment can be made.

Role of Office of IOT&E and IOT&E Team in COI Development. Due to the important role COIs play in system tests and operational assessments, and due to problems created by inadequate COIs, the Office of IOT&E will work with the service organization to assist in the development of a complete set of testable COIs. COIs should reflect high-level operational requirements and should avoid including "issues of the day." COIs used in the test plans by the service organization and the IOT&E program manager should be those defined in the Exhibit 300 Program Baseline, Attachment 1: Program Requirements.

New Content: Test and Evaluation Process Guidelines:
D2 IOT&E Team

Organizations that operate, maintain, or are otherwise operationally affected by the implementation of a new system are represented on the IOT&E team. IOT&E teams will include subject-matter experts at both the working level and supervisory levels from Headquarters and field operations.

The Office of Safety Assurance coordinates with appropriate ATO offices to obtain IOT&E team members from field facilities. Additional participants may include non-FAA personnel who are system users such as the National Weather Service, and employees of the Department of Defense.

Office of Safety Assurance's Role in IOT&E. The IOT&E program manager from the Office of Safety Assurance leads and provides full administrative support to the IOT&E team during IOT&E. The Office of Safety Assurance facilitates the final IOT&E team system assessment by ensuring proper collection, analysis, and reporting of results. The IOT&E team reports the operational assessment of the evaluated system to the in-service decision authority. The Manager of the Office of Safety Assurance represents independent test and evaluation within the FAA.

IOT&E Team Responsibility. The IOT&E team is responsible for conducting independent operational assessments of designated programs. Although every attempt will be made to keep members' management informed of assessments and recommendations, IOT&E team assessments and/or recommendations will be based solely on the analyses of system performance and capabilities during IOT&E and of data collected during earlier test phases.

Role of IOT&E Team During System Test and Field Familiarization. IOT&E may use the results from selected SI system test events to aid the resolution of COIs. Members from the IOT&E team observe selected system test events and have access to all system test and PTR data so that a complete IOT&E assessment can be made.

Role of Office of Safety Assurance and IOT&E Team in COI Development. Due to the important role COIs play in system tests and operational assessments, and due to problems created by inadequate COIs, the Office of Safety Assurance will work with the service organization to assist in the development of a complete set of testable COIs. COIs should reflect high-level operational requirements and should avoid including "issues of the day." COIs used in the test plans by the service organization and the IOT&E program manager should be those defined in the Program Requirements Document.

Red Line Content: Test and Evaluation Process Guidelines:
D2 IOT&E Team

Organizations that operate, maintain, or are otherwise operationally affected by the implementation of a new system are represented on the IOT&E team. IOT&E teams will include subject-matter experts at both the working level and supervisory levels from Headquarters and field operations.

The Office of ~~IOT&E~~***Safety Assurance*** coordinates with appropriate ATO offices to obtain IOT&E team members from field facilities.~~-~~ Additional participants may include ***non-***FAA personnel who are system users such as the National Weather Service, and ***employees of*** the Department of Defense.

Office of ~~IOT&E~~*Safety Assurance*'s Role in IOT&E. The IOT&E program manager from the Office of ~~IOT&E~~***Safety Assurance*** leads and provides full administrative support to the IOT&E team during IOT&E. The Office of ~~IOT&E~~***Safety Assurance*** facilitates the final IOT&E team system assessment by ensuring proper collection, analysis, and reporting of ~~test~~ results. The IOT&E team reports the operational assessment of the evaluated system to the in-service decision authority. The ~~Director~~***Manager*** of the Office of ~~IOT&E~~***Safety Assurance*** represents independent test and evaluation within the FAA.

IOT&E Team Responsibility. The IOT&E team is responsible for conducting independent operational assessments of designated programs. Although every attempt will be made to keep members' management informed of assessments and recommendations, IOT&E team assessments and/or recommendations will be based solely on the analyses of system performance and capabilities during IOT&E and of data collected during earlier test phases.

Role of IOT&E Team During System Test and Field Familiarization. IOT&E may use the results from selected SI system test events to aid the resolution of COIs. Members from the IOT&E team observe selected system test events and have access to all system test and PTR data so that a complete IOT&E assessment can be made.

Role of Office of ~~IOT&E~~*Safety Assurance* and IOT&E Team in COI Development. Due to the important role COIs play in system tests and operational assessments, and due to problems created by inadequate COIs, the Office of ~~IOT&E~~***Safety Assurance*** will work with the service organization to assist in the development of a complete set of testable COIs. COIs should reflect high-level operational requirements and should avoid including "issues of the day." COIs used in the test plans by the service organization and the IOT&E program manager should be those defined in the ~~Exhibit 300 Program Baseline, Attachment 1:~~ Program Requirements ***Document***.

D.3 Relationship with Service Organizations

Old Content: Test and Evaluation Process Guidelines:
D.3 Relationship with Service Organizations

IOT&E program managers are extended, non-voting members of service organizations. They attend all pertinent service organization activities and work closely with the service organizations regarding IOT&E and the early identification of operational issues and risks during the monitoring process. The IOT&E team is provided access to SI system test documentation, which it reviews and on which it provides comments. The service organization may coordinate with the IOT&E PM if they would like to have a representative observe IOT&E. During IOT&E, the service organization may decide to withdraw the system if further development and/or corrective action is required before IOT&E proceeds.

Test Working Groups (TWGs). IOT&E program managers/and Office of IOT&E support staff participate on service organization TWGs. This participation facilitates a full understanding by Office of IOT&E of the service organization's test strategy and a full understanding by the service organization of the IOT&E strategy.

Operational Capabilities Tests and Demonstrations (OCTs, OCDs). To ensure that independence is maintained, the Office of IOT&E does not participate directly in OCDs or OCTs. Office of IOT&E personnel are present as observers, but do not have a role on the technical evaluation teams.

New Content: Test and Evaluation Process Guidelines:
D.3 Relationship with Service Organizations

IOT&E program managers should attend all pertinent service organization activities and work closely with the service organizations regarding IOT&E and the early identification of hazards/risks during the monitoring process. The IOT&E team is provided access to SI system test documentation, which it reviews and on which it provides comments. During IOT&E, the service organization may decide to withdraw the system if further development and/or corrective action is required before IOT&E proceeds.
Safety Assurance Interaction with Test Work Groups. For programs with an established Test Work Group (TWG), PMs are encouraged to participate. This helps the

Office of SA understand the Service Team’s test strategy, and it helps the Service Team understand IOT&E strategy, particularly as it applies to COI assessment and multiple IOT&E activities. Participation in the TWG allows the PM to share Lessons Learned from previous IOT&Es and to be involved in reviewing documents produced by the TWG members. Participation also ensures that IOT&E resource requirements are explained.

SA Involvement with Operational Capability Tests and Operational Capability Demonstrations. The Office of SA may monitor Operational Capability Tests and Operational Capability Demonstrations, system evaluations conducted prior to contract award, and R&D demonstrations of designated programs. To maintain its independence, the Office of SA does not directly participate in these activities, but instead monitors them to identify potential safety hazards and possible areas of improvement in the evaluation process.

Red Line Content: Test and Evaluation Process Guidelines:
D.3 Relationship with Service Organizations

IOT&E program managers ~~are extended, non-voting members of service~~***should*** ~~organizations. They~~ attend all pertinent service organization activities and work closely with the service organizations regarding IOT&E and the early identification of ~~operational issues and~~ ***hazards/***risks during the monitoring process. The IOT&E team is provided access to SI system test documentation, which it reviews and on which it provides comments.~~ The service organization may coordinate with the IOT&E PM if they would like to have a representative observe IOT&E.~~ During IOT&E, the service organization may decide to withdraw the system if further development and/or corrective action is required before IOT&E proceeds.
Safety Assurance Interaction with **Test** ~~**Working**~~***Work*** **Groups*****. For programs with an established Test Work Group*** (~~TWGs~~***TWG***)***, PMs are encouraged to participate***. ~~IOT&E~~ ~~program~~***This*** ~~managers/and~~***helps the*** Office of ~~IOT~~***SA understand the Service Team***&~~amp~~***#8217***;~~E support~~***s test*** ~~staff~~***strategy,*** ~~participate on service organization~~***and it helps the*** ~~TWGs.~~***Service*** ~~This~~***Team understand IOT&E strategy,*** ~~participation facilitates a full understanding by Office of~~***particularly as it applies to COI assessment and*** ***multiple*** IOT&E ~~of~~***activities. Participation in*** the ~~service~~***TWG*** ~~organization~~***allows the PM to share Lessons Learned from previous IOT***&~~#8217~~***amp***;~~s test strategy~~***Es and to*** ~~and~~***be involved in*** ~~a full understanding~~***reviewing documents produced*** by the ~~service~~***TWG*** ~~organization~~***members.*** ~~of the~~***Participation also*** ***ensures that*** IOT&E ~~strategy~~***resource requirements are explained***.

SA Involvement with **Operational** ~~**Capabilities**~~***Capability*** **Tests and** ~~**Demonstrations**~~***Operational*** ~~**(OCTs,**~~***Capability*** ~~**OCDs)**~~***Demonstrations*****.** ~~To~~ ~~ensure that independence~~***The Office of*** ~~is~~***SA may monitor*** ~~maintained~~***Operational Capability Tests and Operational Capability Demonstrations***, ~~the Office of~~***system evaluations conducted*** ~~IOT~~***prior to contract award, and R***&~~E does not participate~~***D demonstrations of designated*** ~~directly~~***programs.*** ~~in OCDs or~~***To maintain its*** ~~OCTs.~~***independence, the*** Office of ~~IOT&E~~***SA*** ~~personnel are present~~***does not directly*** ~~as~~***participate in these***

~~observers~~***activities***, but ~~do~~***instead*** ~~not have a role on~~***monitors them to identify potential*** ~~the~~***safety hazards and possible*** ~~technical~~***areas*** ***of improvement in the*** evaluation ~~teams~~***process***.

D.4 IOT&E Designation Process

Old Content: Test and Evaluation Process Guidelines:
D.4 IOT&E Designation Process

Key elements in the process for assigning an IOT&E program designation include:

- Potential programs for IOT&E designation are reviewed by an IOT&E Designation Board. The IOT&E Designation Board consists of Directors of En Route and Oceanic Safety and Operational Support, Terminal Safety and Operational Support, Flight Services Safety and Operational Support, Technical Operations Support, Systems Operations and Safety, and the Office of IOT&E. The Board's review of programs results in a recommendation to the Vice President of Safety Services on IOT&E program designation. This IOT&E Designation Board will commit to providing sufficient resources to support the recommended program designations.
- The Board ensures that priorities are assigned based on factors such as complexity, criticality, acquisition cost, and risk.
- Program designation decisions will be re-verified at key program milestones.

New Content: Test and Evaluation Process Guidelines:
D.4 IOT&E Designation Process

Prior to convening the IOT&E designation board, representatives from each organization meet to discuss the programs and recommendations. The IOT&E designation process is conducted at least once a year and is scheduled to support FAA and Office of Safety Assurance budget development. Figure 1 depicts the IOT&E designation process.

- The Office of SA's Designation Lead manages the designation process by adhering to the following process:
- The Office of SA conducts a review of new and existing acquisition programs, as well as any additional activities requested by the Vice President of the Office of Safety or Designation Working Group. Acquisition program information is garnered from other sources, such as readiness decisions, Joint Resources Council (JRC) readiness meeting minutes, and Office of Management and Budget Exhibits 300.
- The Office of SA prepares program information sheets (see template) that include designation recommendations based on the program review.
- The Office of SA updates all existing Program Management Plans (PMPs) (at a minimum, the Resources section) (see PMP template). The Designation Lead and an SA budget Point of Contact (POC) analyze the resource estimates in the

updated PMPs against the projected activities associated with anticipated program designation and IOT&E strategies; as necessary, the Office of SA develops resource mitigation strategies.

- Representatives from the IOT&E Designation Board's member organizations review the information package and develop recommendations for the Designation Board to review.
- If resources are not sufficient, the IOT&E Designation Board prioritizes recommendations based on potential complexity, criticality, acquisition cost, and hazards, so that the Vice President of the Office of Safety can make decisions on IOT&E designation relative to Office of SA staffing and funding levels.
- The IOT&E Designation Board reviews the program information and makes recommendations to the Vice President of the Office of Safety concerning IOT&E program designation and designated program priorities. The Vice President of the Office of Safety approves or modifies the recommendations.
- The Vice President of the Office of Safety sends a decision memorandum identifying all programs designated for IOT&E to the Vice Presidents of the operational Service Units and also provides a copy to the Office of Aviation Safety.
- Program designation decisions are reviewed at key program milestones. A decision to increase or decrease the level of IOT&E activity can be made at these times.
- If the Vice President of the Office of Safety removes a program from IOT&E designation, the Office of SA prepares a decision memorandum to be signed by the Vice President of the Office of Safety.

Figure D4-1: IOT&E Designation Process

Red Line Content: Test and Evaluation Process Guidelines:

D.4 IOT&E Designation Process

~~Key elements in~~***Prior to convening*** the ~~process for assigning an~~ IOT&E ~~program~~ designation ~~include: Potential~~***board, representatives from each organization meet to discuss the*** programs ~~for~~***and recommendations. The*** IOT&E designation ~~are reviewed by~~***process is conducted*** ~~an~~***at least once a year and is scheduled to support FAA and Office of Safety Assurance budget development. Figure 1 depicts the*** IOT&E ~~Designation Board~~***designation process***.

- The ~~IOT~~***Office of SA***&~~amp~~***#8217***;~~E~~***s*** Designation ~~Board~~***Lead*** ~~consists~~***manages*** ~~of~~***the designation process by adhering to the following process:***
- ***The*** ~~Directors~~***Office*** of ~~En~~***SA*** ~~Route and Oceanic Safety~~***conducts a review of new*** and ~~Operational~~***existing acquisition*** ~~Support~~***programs***, ~~Terminal~~***as*** ~~Safety and Operational~~***well as any*** ~~Support,~~***additional activities requested by the Vice***

President of the ~~Flight Services~~***Office of*** Safety ~~and~~***or Designation Working Group. Acquisition program*** ~~Operational~~***information*** ~~Support~~***is garnered from other sources***, ~~Technical~~***such as*** ~~Operations Support~~***readiness decisions***, ~~Systems~~***Joint*** ~~Operations and~~***Resources Council*** ~~Safety~~***(JRC) readiness meeting minutes***, and ***Office of Management and Budget Exhibits 300.***

- ***The Office of SA prepares program information sheets (see template) that include designation recommendations based on*** the ***program review.***
- ***The*** Office of ***SA updates all existing Program Management Plans (PMPs) (at a minimum, the Resources section) (see PMP template). The Designation Lead and an SA budget Point of Contact (POC) analyze the resource estimates in the updated PMPs against the projected activities associated with anticipated program designation and*** IOT&E ***strategies; as necessary, the Office of SA develops resource mitigation strategies***.
- ***Representatives from the IOT***&~~#160~~***amp***;~~The~~***E Designation*** Board's ***member organizations*** review ~~of programs results in~~***the information package and*** ~~a~~***develop recommendations for the Designation*** ~~recommendation~~***Board*** to ***review.***
- ***If resources are not sufficient, the IOT&E Designation Board prioritizes recommendations based on potential complexity, criticality, acquisition cost, and hazards, so that*** the Vice President of ***the Office of*** Safety ~~Services~~***can make decisions*** on IOT&E ~~program~~ designation~~.~~ ***relative to Office of SA staffing and funding*** ~~This~~***levels.***
- ***The*** IOT&E Designation Board ~~will commit to providing sufficient~~***reviews the program information and*** ~~resources~~***makes recommendations*** to ~~support~~***the Vice President of*** the ~~recommended~~***Office of Safety concerning IOT&E program designation and designated*** program ~~designations~~***priorities. The Vice President of the Office of Safety approves or modifies the recommendations***.
- The ~~Board~~***Vice*** ~~ensures that priorities are assigned based on factors such as~~***President of the Office of Safety sends a decision memorandum*** ~~complexity,~~***identifying*** ~~criticality,~~***all*** ~~acquisition~~***programs*** ~~cost,~~***designated for IOT&E to the Vice Presidents of the operational Service Units*** and ~~risk~~***also provides a copy to the Office of Aviation Safety***.
- Program designation decisions ~~will be~~***are*** ~~re-verified~~***reviewed*** at key program milestones. ***A decision to increase or decrease the level of IOT&E activity can be made at these times.***
- ***If the Vice President of the Office of Safety removes a program from IOT&E designation, the Office of SA prepares a decision memorandum to be signed by the Vice President of the Office of Safety.***

-

-

Figure D4-1: IOT&E Designation Process

D.5 IOT&E Method of System Assessment

Old Content: Test and Evaluation Process Guidelines:

D.5 IOT&E Method of System Assessment

The assessment of the operational readiness of the system will be performed by the IOT&E team after IOT&E. The system will be assessed for operational readiness based on the operational issues associated with the COIs. The IOT&E team may not be able to fully evaluate all operational aspects of the system during IOT&E due to limitations that may be site-specific, part of the operational environment, or that otherwise prevent the collection of enough relevant information.

Issue Risk Assessment

The evaluation process begins by correlating the collected data from system test, field familiarization, and IOT&E with the COI/MOEs/MOSs to verify that all operational requirements have been assessed. There will be a data trail from the data elements/MOPs to the MOEs/MOSs, and in turn, to the corresponding COIs.

The IOT&E team will analyze the data to identify issues and categorize them as either operational risk issues or comments. Identified operational issues will then be assessed for operational risk using the process described below.

Operational Risk Issues: The risk ratings for these issues will be based on the consensus of the IOT&E team members and will be supported by data that will have been collected during the evaluation, and, if applicable, data collected during earlier testing. The level of risk will be determined by assessing both the operational impact and frequency of occurrence using the following definitions:

Operational Impacts

The operational impacts are defined as follows:

> **CRITICAL** – A problem that will prevent, degrade, or interrupt operational service or jeopardize safety, and has no acceptable workaround.
>
> **MAJOR** – A problem that will —
>
>> a) prevent, degrade, or interrupt operational service or jeopardize safety, but has an acceptable workaround; or
>>
>> b) disable a support system function that is essential to operational or system performance analysis, and has no acceptable workaround.

MINOR – A problem that presents a level of operational impact not covered by the critical or major categories above.

Frequency of Occurrence

The frequency of occurrence is defined as follows:

OFTEN – A problem that repeatedly occurred while the system/service was operational within the NAS and is very likely to recur when the causal conditions exist.

OCCASIONAL – A problem that intermittently occurred while the system/service was operational within the NAS and is likely to recur when the causal conditions exist.

ISOLATED – A problem that rarely occurred while the system/service was operational within the NAS or only occurred during any type of operational testing. The likelihood of recurrence is minimal or the specific causal conditions have not been determined.

The following table illustrates the relationship of operational impact to frequency of occurrence in the assessment of operational risk:

		OPERATIONAL IMPACT		
		MINOR	MAJOR	CRITICAL
FREQUENCY OF OCCURRENCE	ISOLATED	**LOW**	**LOW/MEDIUM***	**MEDIUM/HIGH***
	OCCASIONAL	**LOW**	**MEDIUM**	**HIGH**
	OFTEN	**LOW/MEDIUM***	**MEDIUM/HIGH***	**HIGH**

* Only one risk rating will be assigned to an issue. It will be based on Team consensus.

Comments: This category would include issues that warrant consideration and are not operational risk issues. Some examples of issues which may fall into this category are: positive comments on system performance, concerns with interfacing systems that are not currently under assessment, required operational capabilities not included in the system under assessment (these should have been addressed in the IOTRD), and resources.

System Assessment

Once the issues have been identified and rated for risk, the system will be assessed for operational readiness based on the assessment of the individual issues. The system will be assessed for operational readiness as follows:

- **Operationally Ready:**

- There are no high risk issues and the combined level of risk of all issues does not preclude operational use.

- **Not Operationally Ready:**

  - There is at least one high risk issue or the combined level of risk of all issues precludes operational use.

IOT&E Results

Results from IOT&E will be documented in an IOT&E report. The report will be distributed to the service organization and all ATO stakeholders at the Directorate and Vice President levels. The report will also be sent to the ATO COO. In the case of joint programs with the Department of Defense, the report will be sent to the appropriate Department of Defense offices.

The IOT&E report will normally be briefed in the week following the report's completion. Briefings are scheduled at the Directorate and Vice President levels for all ATO stakeholders and the service organization. A briefing is also scheduled for key site managers. The briefing series may be tailored as appropriate for the program.

New Content: Test and Evaluation Process Guidelines:

D.5 IOT&E Method of System Assessment

The evaluation process will begin by correlating the collected data from DT, OT, Field Familiarization, and IOT&E with the COIs/MOEs/MOSs to verify that all operational requirements have been assessed (see paragraph 4.3.1 for a description of COI/MOE/MOS decomposition). There is a data trail from the Data Elements/MOPs to the MOEs/MOSs, and in turn, to the corresponding COIs and the hazards identified in the SRMD (if applicable).

The IOT&E Team will analyze the data to identify problems and categorize them as either operational hazards or comments. Identified operational hazards will then be assessed for operational risk using the process described below.

Operational Hazard Assessment

Documenting an IOT&E hazard involves the first nine steps of the Preliminary Hazard Analysis, which is depicted in the figure below.

Figure D.5-1: Preliminary Hazard Analysis

Definitions of Severity

The IOT&E Team will assess the severity of each hazard using the following matrix:

Figure D.5-2: Definitions of Severity

Comments: This category would include issues that warrant consideration and are not operational risk issues. Some examples of issues which may fall into this category are: positive comments on system performance, concerns with interfacing systems that are not currently under assessment, required operational capabilities not included in the system under assessment (these should have been addressed in the IOTRD), and resources.

System Assessment

Once the issues have been identified and rated for risk, the system will be assessed for operational readiness based on the assessment of the individual issues. The system will be assessed for operational readiness as follows:

- **Operationally Ready:**

  - There are no high risk issues and the combined level of risk of all issues does not preclude operational use.

- **Not Operationally Ready:**

  - There is at least one high risk issue or the combined level of risk of all issues precludes operational use.

IOT&E Results

Results from IOT&E will be documented in an IOT&E report. The report will be distributed to the service organization and all ATO stakeholders at the Directorate and Vice President levels. The report will also be sent to the ATO COO. In the case of joint programs with the Department of Defense, the report will be sent to the appropriate Department of Defense offices.

The IOT&E report will normally be briefed in the week following the report's completion. Briefings are scheduled at the Directorate and Vice President levels for all ATO stakeholders and the service organization. A briefing is also scheduled for key site managers. The briefing series may be tailored as appropriate for the program.

Red Line Content: Test and Evaluation Process Guidelines:
D.5 IOT&E Method of System Assessment

The ~~assessment of the operational readiness of the system will be performed by the IOT&E team after IOT&E. The system will be assessed for operational readiness based on the operational issues associated with the COIs. The IOT&E team may not be able to fully evaluate all operational aspects of the system during IOT&E due to limitations that may be site-specific, part of the operational environment, or that otherwise prevent the collection of enough relevant information. Issue Risk Assessment The~~ evaluation process ~~begins~~***will begin*** by correlating the collected data from ~~system~~***DT,*** ~~test~~***OT***, ~~field~~***Field*** ~~familiarization~~***Familiarization***, and IOT&E with the ~~COI~~***COIs***/MOEs/MOSs to verify that all operational requirements have been assessed ***(see paragraph 4***.***3.1 for a description of COI/MOE/MOS decomposition).*** ~~There will be~~***There is*** a data trail from the ~~data~~***Data*** ~~elements~~***Elements***/MOPs to the MOEs/MOSs, and in turn, to the corresponding COIs ***and the hazards identified in the SRMD (if applicable)***.

The IOT&E ~~team~~***Team*** will analyze the data to identify ~~issues~~***problems*** and categorize them as either operational ~~risk issues~~***hazards*** or comments. Identified operational ~~issues~~***hazards*** will then be assessed for operational risk using the process described below.

Operational ~~Risk~~*Hazard* ~~Issues:~~*Assessment* ~~The risk ratings for these issues will be based on the consensus of~~

Documenting ~~the~~***an*** IOT&E ~~team members and will be supported by data that will have been collected during the evaluation, and, if applicable, data collected during earlier testing. The level of risk will be determined by~~***hazard*** ~~assessing~~***involves*** ~~both~~ the ~~operational impact~~***first*** ~~and frequency~~***nine steps*** of ~~occurrence using~~ the ~~following definitions: Operational Impacts The operational impacts are defined as follows: CRITICAL – A problem that will~~***Preliminary*** ~~prevent,~~***Hazard*** ~~degrade~~***Analysis***, ~~or interrupt operational service or jeopardize~~***which*** ~~safety,~~***is*** ~~and has no acceptable workaround~~***depicted in the figure below***.

~~MAJOR – A problem that will – a) prevent, degrade, or interrupt operational service or jeopardize safety, but has an acceptable workaround; or~~

~~b) disable a support system function that is essential to operational or system performance analysis, and~~***Figure*** **~~has~~*****D.5-1:*** **~~no acceptable~~*****Preliminary Hazard*** **~~workaround.~~*****Analysis***

~~MINOR~~

~~– A problem that presents a level of operational impact not covered by the critical or major categories above.~~

~~Frequency~~***Definitions*** **of** **~~Occurrence~~*****Severity***

The ~~frequency of occurrence is defined as follows: OFTEN~~ ***IOT***&~~#8211~~***amp***;~~ A problem that repeatedly occurred while the system/service~~***E*** ~~was operational within~~***Team will assess*** the ~~NAS and is very~~***severity*** ~~likely to recur when~~***of each hazard using*** the ~~causal conditions~~***following*** ~~exist.~~***matrix:***

~~OCCASIONAL~~

~~– A problem that intermittently occurred while the system/service was operational within the NAS and is likely to recur when the causal conditions exist.~~

~~ISOLATED – A problem that rarely occurred while the system/service was operational within the NAS or only occurred during any type of operational testing.~~

~~The likelihood of recurrence is minimal or the specific causal conditions have not been determined.~~

~~The following table illustrates the relationship of operational impact to frequency of occurrence in the assessment of operational~~***Figure*** **~~risk~~*D.5-2*: ~~– OPERATIONAL IMPACT MINOR MAJOR CRITICAL FREQUENCY~~**_Definitions_ **~~OF~~*of* ~~OCCURRENCE ISOLATED LOW LOW/MEDIUM* MEDIUM/HIGH* OCCASIONAL LOW MEDIUM HIGH~~**_Severity_

~~OFTEN LOW/MEDIUM*~~

~~MEDIUM/HIGH*~~
~~HIGH~~

~~* Only one risk rating will be assigned to an issue. It will be based on Team consensus.~~

Comments: This category would include issues that warrant consideration and are not operational risk issues. Some examples of issues which may fall into this category are: positive comments on system performance, concerns with interfacing systems that are not currently under assessment, required operational capabilities not included in the system under assessment (these should have been addressed in the IOTRD), and resources.

System Assessment

Once the issues have been identified and rated for risk, the system will be assessed for operational readiness based on the assessment of the individual issues. The system will be assessed for operational readiness as follows:

- **Operationally Ready:**

  - There are no high risk issues and the combined level of risk of all issues does not preclude operational use.

- **Not Operationally Ready:**

  - There is at least one high risk issue or the combined level of risk of all issues precludes operational use.

IOT&E Results

Results from IOT&E will be documented in an IOT&E report. The report will be distributed to the service organization and all ATO stakeholders at the Directorate and Vice President levels. The report will also be sent to the ATO COO. In the case of joint programs with the Department of Defense, the report will be sent to the appropriate Department of Defense offices.

The IOT&E report will normally be briefed in the week following the report's completion. Briefings are scheduled at the Directorate and Vice President levels for all ATO stakeholders and the service organization. A briefing is also scheduled for key site managers. The briefing series may be tailored as appropriate for the program.