

FAQ

'FREQUENTLY ASKED QUESTIONS'

1. Is Software Blocking (SWB) (now Capability Set) for all Army systems or just C2 systems?

SWB is for all Army systems with C2 interoperability requirements; the Army systems with IT/NSS capabilities must undergo an Army Interoperability Certification (AIC). The Army CIO/G-6 can grant exemptions if an Army system doesn't have any interoperability requirements. AIC tests the ability of IT/NSS systems to successfully digitally exchange secure and timely data, information, and services, to enable them to operate effectively and efficiently together, thus achieving system of systems (SoS) interoperability.

2. Is AIC additive to developmental testing (DT), operational testing (OT) and Joint Interoperability Test Command (JITC) requirements?

AIC is part of DT, one of the block checks required for a milestone decision IAW AR 70-1 and other DoD 5000 regulations. An AIC should occur before a system enters Initial Operational Test and Evaluation or IOT&E.

3. Can contractors troubleshoot and fix their systems during test?

Yes, but the contractors are designated as technicians/engineers and if the fix is beyond what the operator (Soldier) could perform, then the issue/fix is documented in a Test Incident Report. No software changes are allowed during an AIC test. The CTSF has implemented a rigorous test-fix-test (TFT) process executed prior to entering into a formal test. This process provides the customer and test officer the time to validate the software's interoperability and the mission threads before entering formal AIC testing. This methodical, measured approach to testing maintains configuration control, yet allows software fixes and additional software drops to facilitate development of interoperable functional code in a shortened timeframe.

4. What is a TIR and how does it affect certification?

TIR stands for Test Incident Report. TIRs document problems that are identified during certification testing. The CTSF's Executive Scoring Conference (ESC) assigns a TIR severity level score to the report. The ESC is comprised of a CTSF rep, a ASA(ALT) rep, and a TRADOC rep. This ensures that the tester, PM, and user rep have input into the scores assigned to a TIR. TIRs are assigned severity levels ranging from level one – the most serious to level five – the least serious. A TIR is marked as a level one if the identified problem could prevent the accomplishment of an essential capability or jeopardize safety, security, or other requirement designated “critical”. A level two TIR represents a problem that adversely affects the accomplishment of an essential capability and no work-around solution is known. A level three TIR represents a problem that adversely affects the accomplishment of an essential capability but a work-around solution is known. A level four TIR represents a problem that results in user/operator inconvenience or annoyance but does not affect a required operational or mission-essential capability. Any other problem is reflected as a level 5 TIR. TIRs are provided back to the PM/PdM for resolution. Systems with unresolved TIRs can still be fielded; this decision is made by the Army G-3/5/7 based on data CTSF provides to the Army CIO/G-6. In a perfect

world, all TIRs are resolved prior to fielding. In practice, a system may still have a few low-level TIRs (3s and 4s) remaining but get fielded anyway because essential functions are not adversely affected or work-arounds are available.

5. If a single system fails certification, what happens to that software (SW) release?

That depends on if it is a new baseline or just an update to the baseline. If a system fails during an update, then the PM makes a SW change and then tests in the next window. If it is a new baseline, individual systems get a certification or non-certification letter from the Army CIO/G-6 and then must have a get well plan or present operational impacts from TRADOC. If it is a new baseline and it is a core system, the core system pays for the new test and the players reassemble (SoS environment). The systems are then re-tested as soon as the major failure has been corrected.

6. What was before SWB1?

There were out of cycle AIC tests that still required a SoS environment, but SW releases were not planned to occur within set windows. The Army instituted SWB in 2001 in order to coordinate, synchronize and enforce interoperability amongst Army systems. Since that time, an increasing number of Army systems, and later non-Army systems, were added to the process. According to the SWB policy, SWB was to be "a balanced and disciplined policy/process for harmonizing requirements and development that leads to fielding and support of software intensive systems. It will ensure that they expedite the rapid delivery of innovative, integrated, and operationally suitable Warfighter capability to the field."

7. Was it by fiscal year (FY) or calendar year (CY) or is SWB1 the first time for this type of release?

SWB1 is not the first release of its kind; there was [Army Battle Command System] ABCS 6.3, 6.3D, 6.4, and finally SWB1. In the past, the releases were referred to as *baselines*, now they are called *capability sets* (CS) (e.g. CS 11-12 follows SWB2+) based on a 2007 decision by the Chief of Staff of the Army. The Army adopted the Capability Set construct which dictates that units will be fielded 'capabilities' (which are provided by a set of systems/software/equipment) as a group or set instead of each Program delivering individual products or product upgrades when they are ready. This approach acknowledges that battle command systems require compatible networks and other infrastructure to achieve optimum utilization. If you field a sophisticated C2 system but do not provide the unit with the transport or power to allow it to work right, you have not fielded them with any usable capability. The capability set construct remedies this by synchronizing delivery of 'capabilities' (software, transport, trained operators, HVAC and power, etc.).

8. What degree of virtualization takes place during AIC?

The CTSF uses as much of the actual LWN/BC hardware as is practical and possible. When not possible or practical, the CTSF uses simulators, including C3 Driver. System engineers are currently working to virtualize certain systems. We expect this effort to expand in the future. Systems that will field with partial virtualization, i.e. the Battle Command Services Server (BCCS) are tested in that configuration, i.e. server hardware with some virtualization components. This is done to represent the to-be-fielded hardware.

9. How is the tri-annual certification linked to SWB?

Tri-annual construct was a collaborative effort between the CTSF, ASA(ALT), and the Army CIO/G-6. The CTSF implemented Tri-annual AIC after presenting the construct to the Dec 2008 Software Blocking Implementation Planning Team (SWB IPT) SWB IPT and now the Tri-annual is policy.

10. How does a system come to the CTSF to test?

The interested PM submits a signed 'request to test' letter to the Army CIO/G-6. The letter must identify exactly what is to be tested: the system and software specifications, and should include requested test dates and locations as well as POC information. Using the information provided in the request to test letter, a CTSF test officer drafts a test concept brief. The brief allows those involved to understand the scope of the test and includes enough information to begin the cost-estimate process. Upon receipt of all system documentation, the CTSF will prepare a comprehensive test plan and coordinate that plan with the Army CIO/G-6, the appropriate TRADOC capability manager, and the Product Manager or PdM. Once the test plan is signed, test costs are determined and provided to the PdM. Thirty days prior to the scheduled test date, the PdM should provide system hardware (if required) and software to the CTSF along with a MIPR to cover the cost of the test.

11. Who can I talk to about borrowing a workspace while I'm on-site?

In most cases, whether initiating any type of AIC testing or requesting other less formal support, contacting an action officer in the CTSF Operations section is a great first step – CTSF Operations – 254.532.8321 ex 2505. Our Operations section will coordinate the request for you or link you up with the staff member best suited to handle your request.

12. How long has the CTSF been in trailers, and are there plans to move into a building?

The CTSF began with a 4-trailor footprint in 1996. Yes, there are plans underway to build a permanent facility on Fort Hood in the 2015-2016 timeframe.

13. What's the difference between the CTSF as an organization and the CTSF as a campus?

The Central Technical Support Facility organization is a 230-person, COL-level directorate organized of military personnel, government civilians, and contractors with a mission to provide a unique scalable environment, with skilled personnel, using qualified processes to support the DoD's net enabled strategic vision by executing configuration management, system of systems integration, and interoperability certification testing for Army and Joint C4I providers. The CTSF campus, on the other hand, houses the CTSF organization as well as approximately 400 representatives from PEOs/PMs, vendors, and the Army staff. These personnel are on-site conducting PEO/PM development, integration, and training.

14. Is there one contract vehicle for the 400 contractors at the CTSF?

No, multiple contract vehicles exist for our contracted work force.

15. What are the primary resources provided by the CTSF to execute SoSI and AIC testing.

In addition to the staff, the CTSF offers three reconfigurable test floors containing Corps- to Battalion-level architectures and three systems of systems engineering laboratories. The CTSF provides a system of systems (SoS) integration lab that allows the PM to assess his system's interoperability in a non-attribution environment prior to AIC. The CTSF also provides network engineers who establish network connectivity in the SoS environment. The CTSF has established connections to disparate networks including the Defense Research and Engineering Network (DREN), Secure Defense Research and Engineering Network (SDREN), and Joint Training and Experimentation Network (JTEN) allowing distributed operations. The CTSF also has a dedicated local BFT Network Operations Center which links celestial and terrestrial platforms to support all baselines for testing and integration events, internal and external to the CTSF.

For more information, contact CTSF Strategic Communications – 254-532-8321 x2611/2600

