DEFENSE BUSINESS SYSTEM MODERNIZATION CERTIFICATION APPROVAL FAQs

1. What does 10 U.S.C. 2222 (as added by section 332 of the Ronald W. Reagan National Defense Authorization Act (NDAA) for Fiscal Year 2005) require in regard to "defense business system modernizations"?

Effective October 1, 2005, any defense business system modernization that will have a total cost in excess of $1M , must be reviewed by the appropriate Office of the Secretary of Defense (OSD) Investment Review Board (IRB), certified by the designated Approval Authority and the certification must be approved by the Defense Business System Management Committee (DBSMC) before any funds for modernization can be obligated.

2. What if funds are obligated without certification and approval required by 10 U.S.C. 2222?

An officer or employee of the United States Government that knowingly and willfully obligates funds for a defense business system modernization that has a total cost over $1M without an approved certification will violate 31 USC 1341(a)(1) (the Anti-Deficiency Act (ADA)). The ADA provides for a fine of up to $5000, and imprisonment for not more than 2 years, or both.

3. What is a "defense business system"?

10 U.S.C. 2222(j)(2) states: The term "**defense business system"** means an information system, other than a national security system, operated by, for, or on behalf of the Department of Defense, including financial systems, mixed systems, financial data feeder systems, and information technology and information assurance infrastructure, used to support business activities such as acquisition, financial management, logistics, strategic planning and budgeting, installations and environment, and human resource management.

Information technology and information assurance infrastructure systems that are intended to be used to support the general activities of the Department and are not intended to be used primarily to support business activities are not defense business systems. This includes local area networks, metropolitan area networks, wide area networks and telephone systems. However, modernizations of such systems that are intended to be used primarily to support business activities shall be treated as defense business system modernizations.

4. What is a "national security system"?

10 U.S.C. 2222(j)(6) states: The term "**national security system"** has the meaning given that term in section 2315 of this title.

10 U.S.C. 2315 states:

(a) For the purposes of subtitle III of title 40, the term "national security system" means those telecommunications and information systems operated by the Department of Defense, the functions, operation, or use of which—

(1) involves intelligence activities;

(2) involves cryptologic activities related to national security;

(3) involves command and control of military forces;

(4) involves equipment that is an integral part of a weapon or weapons system; or

(5) subject to subsection (b) is critical to the direct fulfillment of military or intelligence missions.

(b) Subsection (a)(5) does not include procurement of automated data processing equipment or services to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

5. What is a "defense business system modernization"?

10 U.S.C. 2222(j)(3) states:

The term "defense business system modernization" means--

(A) the acquisition or development of a new defense business system; or

(B) any significant modification or enhancement of an existing defense business system (other than necessary to maintain current services).

Note: The type of funds will not always be an accurate indicator of a defense business system modernization. For example, although most efforts using Operation and Maintenance funds would be for the purpose of maintaining current services and therefore would not be a modernization, some efforts that use such funds may be for acquisition of a new system or significant enhancement of an existing system.

6. What is a "significant" modification or enhancement of an existing system?

The term "significant" means in excess of $1M in total cost of the modernization.

7. Do Commercial off-the-shelf (COTS) acquisitions require certification?

Yes.

8. Do technical refreshments or other system upgrades require certification approval?

Generally, technical refresh or system upgrades do not require certification if the current level of service is being maintained but not significantly enhanced and changes are being made primarily to reduce technical risk or reduce operational costs. For example, a) replacing software, systems

or infrastructure that is no longer being supported, or b) making upgrades to improve security or meet information assurance requirements, or c) making changes that reduce operating and maintenance costs do not require certification approval. However, if the technical refreshment or system upgrade is part of a larger modernization effort that expands or significantly enhances service and capabilities, then technical refreshment and other system upgrade costs should be included in the overall modernization cost and included in the certification submission.

9. Does the $1M threshold apply to the annual cost of a modernization or the total cost of the modernization or the life cycle cost of all program modernizations?

The $1M threshold is based on the total cost of the modernization from concept refinement phase, or pre-initiation phase, to deployment (but not including operation and support (i.e., sustainment phase)). Depending on how the modernization is structured, it may be a one-year effort or a multi-year effort and may extend beyond the FYDP. A certification approval will generally apply to that portion or phase of the modernization for which procurement and funding authority has been granted.

10. If several system changes are planned, is it better to bundle them and submit them as one initiative or to submit several certification packages?

It is recommended that programs submit a single certification package that covers the full scope, cost and schedule for the entire modernization effort, rather than to submit several certification packages that divide up the modernization. The bundled submission provides a more accurate representation of the scope, cost, and schedule of the modernization.

11. Can I spend up to $1M before I get IRB and DBSMC certification and approval?

No. Certification by the approving authority and approval by the DBSMC is required before obligating any modernization, even if the cost in the first year will be less than $1M.

12. What happens if the program spends $1.00 more than was approved?

Generally, the certification will allow for expenditures up to ten percent (10%) more than the approved amount. For example if a program was approved to obligate $5M over three years, the program could spend up to $5.5M without getting recertified. The additional 10% applies to the entire period. For example, a program could spend $2M, $2M, $1.5M over three years, or $3M, $2M, $.5M; as long as it did not exceed $5.5M over three years it would not require recertification. However, if the reason the program is over-spending is due to under performance (rather than accelerated deployment), the program could have its certification rescinded by the IRB. This is the sort of situation that would be assessed during the program's annual investment review.

13. What is an annual investment review?

The annual Investment Review Process is required by 10 U.S.C. 2222(g). This review will be performed at various levels – within the Components and at the IRB level. It will be used to monitor compliance, cost, schedule, performance, and implementation progress and program effectiveness. For Tier 1 programs (MAIS or MDAP), the annual review will be conducted in conjunction with the annual Defense acquisition process in-process review.

14. Is there a certification document?

Yes. The terms and conditions of the certification approval will be documented in the IRB recommendation for certification memorandum that will be submitted to the Certification Authority (referred to as the Approval Authority in 10 U.S.C. 2222). The Certification Authority may also apply conditions to a program beyond those recommended by the IRB, if so those conditions would be described in the Certification Authority's request for certification approval memorandum sent to the DBSMC. Copies of all memorandums will be available on the IRB portal.

15. What information is contained in the approval memoranda?

The Certification Authority memorandum and the DBSMC certification approval memorandum provide authority to obligate funds for the modernization and define the scope, funding amount, schedule and, in some cases, specific conditions under which the funds may be obligated.

16. How long does the certification approval last?

Certification approvals last for the duration of the modernization as long as scope, cost and schedule are maintained and any conditions contained in the approval letter are met. Recertification is required when additional capital investment in excess of 10% of the approved amount or additional time in excess of 10% of the approved time is required to complete the development or modernization. The program and PCA must determine the most appropriate time period to request obligation authority for. However, it is possible that either an IRB, an Certification Authority, or the DBSMC may rescind an approval for any of a number of reasons, such as poor performance, schedule slippage, or redundancy to other DoD Enterprise capabilities.

17. What happens if the program does not comply with the terms of the approval memoranda?

Failure to comply with the terms of the approval letter may result in a rescinding of the approval or a requirement to recertify. It may also result in the withholding of program funding until the conditions are met. 10 U.S.C. 2222 requires every defense business system to be reviewed periodically, at least annually, by an IRB. This means that although a systems modernization certification may be required only once during the life cycle of the modernization, the program or system will be reviewed at least annually by an IRB to ensure the planning, design,

acquisition, development, deployment, operation, maintenance, modernization, and project cost benefits and risks of the defense business systems are consistent with the Department's requirements.

18. How does a program get certification approval?

Program Managers (PM) must submit required certification documentation to their designated Pre-Certification Authorities (PCAs). The PCAs will review their submissions and if they approve of the modernization, they will prepare a PCA certification recommendation and forward it with all required documentation to the appropriate IRB via the OSD IRB Portal.

19. Where do I get information that explains how to submit a business system certification package?

Detailed information regarding certification package submission requirements is available at the Department of Defense Investment Review Board (IRB) Portal (https://portal.acq.osd.mil/portal/server.pt). General information is also available at the Business Management Modernization Program (BMMP) web-site (https://spsbmmp.dfas.mil) and BMMP portal (http://www.dod.mil/comptroller/bmmp/pages/index.html) . Service or Agency business system investment Pre-Certification Authorities (PCAs) (usually the Chief Information Officer (CIOs)) are also likely to have information regarding Component specific requirements.

Access to the IRB Portal is password restricted. Each IRB has a mailbox account. To establish a portal account and obtain login information, contact the IRB mailbox and identify name, organization, phone number, and email address.

FM: FM.IRB@OSD.MIL
WSLM/MSSM: Walter Schneider, walter.schneider.ctr@osd.mil, SCST, 614-3883x126; Mark Warren, SCST, mark.warren.ctr@osd.mil, 614-3883x126
RPILM: Tracy DeBusk, tracy.debusk.ctr@osd.mil
HRM: Jeanette S. Whiten, jeanette.whiten@osd.pentagon.mil; James A. Messing, jim.messing.ctr@osd.pentagon.mil

20. How long does it take to get a DBSMC decision?

The DBSMC meets monthly. All programs that were certified by a Certification Authority during the preceding month will be presented to the DBSMC during that month's meeting. IRBs meet monthly, all programs that have been pre-certified by their PCA and submitted 2 weeks prior to the IRB date will be presented to the IRB. Overall IRB/DBSMC processing time is about 30 days from the time a certification package is received from the Component PCA. MAIS and MDAP program certifications are tied to the Defense Acquisition process.

21. What is the role of the Pre-Certification Authority (PCA)?

Each Component has a designated PCA. The PCA reviews business system investments and "pre-certifies" that they are consistent with the Component's Business Systems Transition Plan and compliant with the Component and/or DoD Business Enterprise Architecture (BEA). They also certify that an economic viability analysis was completed and reviewed by the program's independent cost review authority for accuracy. If they find the program meets certification criteria, they "pre-certify" the system as compliant and forward the certification package to the appropriate IRB for processing through the DBSMC for approval.

22. Who are the IRBs?

Financial Management (FM)
Human Resources Management (HRM)
Real Property & Installation Lifecycle Management (RPILM)
Weapon Systems & Material Supply Management (WS&MSM)

23. What is the role of the IRB?

IRBs review business system Investment Technology (IT) submission packages and make certification recommendations based on the PCA's review and their own assessment. The IRBs are responsible for coordinating with other IRBs for systems that perform multiple capabilities and cross core business mission areas. They will consider whether the system supports a justified need (e.g. satisfies a policy, law or regulation or provides required capabilities) and has a sound business case (e.g. provides significant benefit and has a good return on investment). Additionally, they will verify that the modernization is consistent with the DoD and Component Transition Plan and aligned to the DoD Business Enterprise Architecture (BEA). Systems may be certified that do not comply in all areas because they are considered critical to national security, address a critical requirement in an area such as safety or security, or they are necessary to prevent a significant adverse effect on a project that is essential. IRB recommendations are passed to the Certification Authority (usually the chair of the IRB) who certifies the investment to the DBSMC for final review and approval.

24. What is the role of the DBSMC?

The DBSMC recommends to the Secretary of Defense policies and procedures necessary to achieve business transformation, reform, reorganization and process improvements within DoD. The DBSMC also reviews and approves any major update to the defense business enterprise architecture (BEA), approves defense business systems modernization plans, manages cross-integration issues, and oversees the IRB process. The DBSMC has final approval authority on all certifications, and addresses appeals or other issues that cannot be resolved at the IRB level.

25. What documents must be submitted by the PCAs to the IRBs?

PCAs are required to submit the following items for each system or bundle of systems to be certified:

- Pre-Certification letter
- Certification Template (Tiers 1 and 2 only)
- Certification Dashboard
- System Investment Summary (Tier 3 only)

The following documents will not be submitted to the IRB but should be available upon request.

- Economic Viability Analysis
- Independent Cost Review Authority

Templates for the above documents are available at the Department of Defense Investment Review Board (IRB) Portal (https://portal.acq.osd.mil/portal/server.pt). Service or Agency business system investment Pre-Certification Authorities (PCAs) (usually the Chief Information Officer (CIOs)) will have information regarding Component specific requirements.

26. What does it mean to be a Tier 1, 2 or 3 system/program?

Tiers were established to define the level of review required based on program cost and importance.

> Tier 1 systems refer to MAIS or MDAP programs or initiatives. They are the highest dollar programs and of the greatest significance.
>
> Tier 2 programs have modernization costs of $10M or more, but are not designated MAIS or MDAP, or they are programs that have been designated as "IRB interest programs" because of their impact on DoD transformation objectives (no dollar threshold).
>
> Tier 3 systems refer to programs with modernization costs greater than $1M but less than $10M.

27. What is the Defense Information Technology Portfolio Repository (DITPR)?

The DITPR was selected by the DoD Chief Information Officer (CIO) as the Enterprise Shared Space for Information Technology (IT) Portfolio Management data for all DoD business IT systems (DCIO Memo, 17 March 2005). The DITPR is a web-based system that provides information about DoD IT systems. Each system in the DITPR has a unique number assigned which facilitates tracking and visibility. The DITPR evolved from the Department of Navy (DON) Application & Database Management System (DADMS) and was

initially selected by the Business Management Modernization Program (BMMP) to support the DoD IT Portfolio Management Review Process. However, DITPR now includes systems from all Mission Areas and has a much broader range of uses including investment review and certification submission support. In late October 2005, the DITPR will also support the Federal Information Security Management Act, E-Authentication, and Privacy Impact Assessment when the DoD IT Registry merges into the DITPR.

28. What is the Information Technology Management Application (ITMA)?

ITMA was an OASD(NII) owned system used to collect and submit the DoD Information Technology Budget. ITMA was merged with the SNaP in 2005 (see FAQ on SNaP-IT) and is now referred to as SNaP-IT. The FY 2006 President's Budget (PB06) was the last collection cycle for the ITMA.

29. What is the Select and Native Programming Data Collection System-Information Technology (SNAP-IT) and what role does it play in the certification process?

SNaP-IT is a OASD(NII) owned system that is used to collect and submit the DoD Information Technology Budget. SNaP-IT is the DoD authoritative database for the Department's Information Technology budget submissions to OMB and Congress; some examples include Capital Investment Reports (OMB Exhibit 300), NDAA Section 352 and 332 Reports, and Information Technology and E-Government Reports (OMB Exhibit 53 and IT-1). The Director, Program Analysis and Evaluation (D,PA&E) operates the SNaP-IT data collection web site that is available at https://snap.pae.osd.mil/snapit/login.aspx. To access SNaP-IT, users must have a PA&E Single Sign-On (PAESSO) account and a SNaP-IT account granted by OASD(NII)/RPBO. SNaP-IT may be used during the Investment Review process to obtain more information on the system's budget profile.

The DCIO is evaluating how to achieve a net-centric solution for IT Budget data; though in the interim theSNaP-IT may provide budget data to update the DITPR financial data. Currently, the information in SNaP-IT and the DITPR is not easily merged because SNaP-IT tracks initiatives, which may/may not encompass a family of systems, whereas the DITPR tracks systems. SNaP-IT assigns an unique number to initiatives, so for a family of systems, multiple systems have the same number. Effective with the Fiscal Year 2007 Budget Estimation Submission (BES07) in August 2005, a defense business system must be reported as an separate initiative. This improvement will provide better visibility of the system budgets and create an alignment with SNaP-IT and DITPR.

30. How do I find out my DITPR or SNaP-IT (formerly ITMA) number?

To determine what your system’s DITPR or SNaP-IT number, contact your component Chief Information Officer’s (CIO) office.

31. Am I required to update information in the DITPR or SNaP-IT?

The Components are required to update both DITPR and SNaP-IT based on guidance from the Deputy Chief Information Officer (CIO). The policy for updating information in the DITPR or SNaP-IT is established by each Component and varies. Program Managers should contact their Component CIO for information regarding their Component's policy regarding access to those systems.

32. How do I get a DITPR account/User ID?

To get a DITPR account:

1) Go to the following URL: https://www.dadms.navy.mil/
2) Click on the **DITPR ACCESS REQUEST** hyperlink below the *DITPR WELCOME* hyperlink.
3) Fill out the New User Request form online.
4) Your account and password should be provided to you within one business day.

33. How do I locate a DITPR number?

1) Go to the following URL: https://www.dadms.navy.mil/
2) Click on the ***DITPR WELCOME*** hyperlink on the left pane.
3) Click on the **DITPR Login** hyperlink on the left pane.
4) Log into DITPR.
5) Enter your User ID and Password.
6) At the Log In Accepted Screen click on Agree
7) Click on the **Search** hyperlink in the upper middle section of the screen above **For Official Use Only (FOUO)**.
8) In the first drop down menu under the gray horizontal bar change the Name option to the system acronym.
9) Click on the gray search button to the right of the text box in which you entered the acronym.
10) DITPR should list the system selected. The DITPR number is listed under the **DITPR ID** caption.