CH 6–1. Purpose
The Defense Acquisition Guidebook (DAG), Chapter 6, provides guidance on where overarching policy may have unique application to the acquisition of Information Technology (IT) in the Department of Defense. The goal is to enable the functional and acquisition communities who are developing and deploying IT capabilities to deploy at the speed at which they become viable — and ensure those capabilities are secure, net-centric, and available to users.

CH 6–2. Background

CH 6–2.1 DoD Information Technology (IT)
The DoD provides the IT infrastructure for our nation’s defenses and the 24/7/365 constant cybersecurity vigilance that is required to defend us from our determined cyber foes.

Historically, DoD’s IT investments were made to meet the needs of individual projects, programs, organizations, and facilities. This decentralized approach resulted in large cumulative costs and a patchwork of capabilities that created cyber vulnerabilities and limited the ability to capitalize on the promise of new developments in IT. That picture is now changing as better enterprise capabilities are being developed and implemented.

“IT” is a large, umbrella term covering many capabilities embodied in computer hardware, software, networking and application hosting services that are essential to warfighting operations and efficient management of warfighting and the Department. Figure 1 depicts some of the types of IT operated in the Department, which are applicable to the topics discussed in Chapter 6. It is not exhaustive of all IT but describes the most common types in the Department.

Figure 1: DoD Information Technology (IT)

CH 6–2.1.1 Key DoD IT Categories
There are varying types of IT managed in the Department though not all are managed in a “traditional” manner through the acquisition process as outlined in the DoDI 5000.02, “Operation of the Defense Acquisition System”. Table 1 explains the broad categories of IT which are acquired and managed under more traditional acquisition structures while Table 2 outlines some exceptions to these processes.

Table 1: IT Managed Under Standard DoD Acquisition Processes
Major Category | Description
--- | ---
Automated Information System (AIS) | As defined in Enclosure 1 Table 1 of DoDI 5000.02 (Footnote 4), an AIS is a system of computer hardware, software, data or telecommunications that performs functions such as collecting, processing, storing, transmitting, and displaying information. AISs exclude hardware and software embedded in a weapons system. Despite minor differences in the definitions, the term “AIS” is synonymous with “IS.” While the word “automated” is historically part of the AIS term, the need for it has greatly diminished now that few people would contemplate an IS that does not take advantage of the automation offered by computer hardware and software. We have now taken to use the term “Information System (IS),” especially when needing to distinguish IS from weapons systems.
Defense Business System (DBS) | As defined in Title 10 U.S.C. section 2222, a DBS is an information system that is operated by, for, or on behalf of the Department of Defense, including any of the following: (i) a financial system; (ii) a financial data feeder system; (iii) a contracting system; (iv) a logistics system; (v) a planning and budgeting system; (vi) An installations management system; (vii) a human resources management system; (viii) a training and readiness system. DBS are not NSS, nor are they systems operated exclusively by the defense commissary system or the exchange system or conducted for the morale, welfare, and recreation of members of the armed forces using non-appropriated funds.
Information Systems (IS) | As defined in Title 44 U.S.C section 3502, an Information System is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information Technology (IT) | As defined in Title 40 U.S.C section 11101, information technology is any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; including computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services, and related resources). IT is equipment used by the DoD directly or is used by a contractor under a contract with the DoD that requires the use of that equipment. This term does not include the definition of National Security Systems as defined in Title 44 U.S.C section 3552.
Major Automated Information System (MAIS) | Per 10 USC 2445a, a MAIS is an AIS that has been so designated by the Milestone Decision Authority (MDA), or meets one or more of the estimated cost magnitude criteria listed in Enclosure 1 Table 1 of DoDI 5000.02.
National Security Systems (NSS) | Defined by the Title 44 U.S.C. section 3552 NSS are telecommunications or information systems operated by or on behalf of the Federal Government, the function, operation, or use of which:
- involves intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system, or, is critical to the direct fulfillment of military or intelligence missions; OR
- is protected at all times by procedures established for information that has been specifically authorized under criteria established by an Executive order or an Act.
CH 6–2.1.2 DoD Information Technology (IT) Acquisition

Acquisition programs are categorized based on the criteria in Enclosure 1 Table 1 of DoDI 5000.02 but are generally categorized based on the cost of the program. CH 1 includes a broader discussion of acquisition categories, or ACATs, and explains the thresholds. In terms of specific applicability to IT programs:

<table>
<thead>
<tr>
<th>Major Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Infrastructure</td>
<td>IT infrastructure is generally non-developmental, commercial-off-the-shelf hardware equipment, and not the subject of its own “acquisition program.” Infrastructure is a critical factor to most if not all IT acquisition programs, however, and more and more is being managed as an integrated facet of the overall program. The cybersecurity posture of a program’s infrastructure is critical. Sometimes, the extent of customization of connected components and integration prompts treatment as an acquisition program, putting it in the category of an Information System. Otherwise, IT infrastructure is acquired as a commodity.</td>
</tr>
<tr>
<td>Embedded IT</td>
<td>Embedded IT (refer to definition of “AIS” in Enclosure 1 Table 1 of DoDI 5000.02 Page 44) is described as computer resources, both hardware and software, that are an integral part of a weapon or weapon system; used for highly sensitive classified programs (as determined by the Secretary of Defense); used for other highly sensitive IT programs; or determined by the Defense Acquisition Executive or designee to be better overseen as a non-AIS program (e.g., a program with a low ratio of RDT&amp;E funding to total program acquisition costs or that requires significant hardware development). This form of IT capability acquisition is usually better managed as a subsystem of the larger weapon system. The embedded IT subsystem PM usually reports to the weapon system PM and in these circumstances oversight of embedded IT programs or subprograms is not distinct from the parent weapon system program.</td>
</tr>
<tr>
<td>Services</td>
<td>Many aspects of IT can be acquired as a service: hardware, software, infrastructure services, and data can all be acquired on a subscription basis, and this form of acquisition is covered by the (new) DoDI 5000.74 “Defense Acquisition of Services.” DoDI 5000.74 applies to programs with “a total estimated acquisition value in current year dollars at or above the simplified acquisition threshold.” If, however, the estimated costs exceed any of the MAIS definition thresholds of DoDI 5000.02Enclosure 1 Table 1 of DoDI 5000.02, the program is treated in the nature of an Information System (MAIS) program.</td>
</tr>
</tbody>
</table>
ACAT I programs are either Major Defense Acquisition Programs (MDAPs) or Major Automated Information Systems (MAIS);

Large IT programs are most often MAIS programs (i.e., they are typically not managed as MDAPs even if they meet the MDAP threshold); and

AIS programs do not fall into the ACAT II category—they are either ACAT I or ACAT III.

Regarding decision authority for IT programs:

The Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)) is the Defense Acquisition Executive (DAE) (or Milestone Decision Authority (MDA)) and will typically review MAIS and MDAP programs as the MDA, unless this authority is delegated.

The Component Acquisition Executive (CAE) or Service Acquisition Executive (SAE) reviews ACAT III programs as the MDA.

The term “Pre-MAIS” (program) used to refer to a MAIS program before it became baselined at Milestone B—a formality previously necessary before it would be recognized as a true “program.” The acquisition community, however, commonly uses the term “program” for an acquisition effort well before it achieves its Milestone B decision. Congress became concerned that this formality was used to avoid some reporting requirements and amended the title 10 USC Chapter 144A MAIS reporting statute to capture “pre-MAIS”. Further evolution in the MAIS oversight community yielded the current term “unbaselined MAIS” for a large AIS program until it achieves a signed (approved) Acquisition Program Baseline, or APB.

Programs may also be deemed special interest for any number of reasons and treated as an MDAP or MAIS—though often these programs are managed in a highly tailored way, and may only be managed as such temporarily.

Many aspects of IT can be acquired as a service; hardware, software, and data can all be acquired on a subscription basis, and this form of acquisition is covered by a recently published DoD 5000.74 “Defense Acquisition of Services.” This policy applies to programs with “a total estimated acquisition value in current year dollars at or above the simplified acquisition threshold.” (See DoD 5000.74 paragraph 2a(2)) If, however, the estimated costs exceed any of the MAIS definition thresholds of DoD 5000.02 the program is treated in the nature of a program (of the MAIS variety) and not a service. (See DoD 5000.74 paragraph 2b(1).)

Additional information on ACAT designations and on MDAP / MAIS categorizations is available from the following resources:

- Title 10 Section 2430 – MDAP
- Title 10 U.S.C. section 2430 – MDAPs
- Title 10 Chapter 144A – MAIS Programs
- DoD 5000.02 (Encl 1, Table 1 Page 44) Enclosure 1 Table 1 of DoD 5000.02 (footnote 4).
- Defense Acquisition University (DAU) Course – Acquisition 101
- CH 1 Section 4.2.3 includes additional discussion on tailoring.

CH 6–3. Business Practice

CH 6–3.1 Oversight and Tailoring

MDA designation and associated oversight is determined by DoDI 5000.02 Enclosure 1 Table 1 of DoDI 5000.02 (Enclosure 1 Table 1) and adjusted through consideration of estimated cost magnitude, risk assessment, third party interest, acquisition phase, subject matter, and system function. This generally applies to programs for acquiring IT, including Information Systems, IT embedded in weapon systems, IT infrastructure, and information services; however, each of those genera of IT acquisition requires a customized (if not unique) approach to structuring the program and providing for its oversight.

From a program structuring / process perspective, the goal should be to design scope a program that will deliver capability rapidly, while tailoring out unneeded or non-value added steps. Tailoring must begin up-front, with key stakeholders involved to create buy-in to the approach. In general, tailoring should consider multiple factors including program size, scope, risk, urgency of need, and technical complexity. IT programs are often excellent candidates for tailoring as they necessitate more rapid deployments and more frequent upgrades of capability.
Generally, the PM proposes and the MDA approves tailoring decisions in an ADM. Tailoring discussions should occur with program leadership, stakeholders, and the MDA (if possible) very early on in the program and should continue throughout. There are various methods of tailoring described throughout this Chapter.

CH 6–3.2 Program Structure

There is no one best way to structure or “tailor” an IT acquisition program. Consistent with applicable statutes and regulations, time constraints for delivery of the capability, solution characteristics, and performance criteria all will determine program strategies and oversight (to include documentation of program information, acquisition phases, timing and scope of decision reviews, and decision levels) to fit the particular conditions of any IT program, similar to weapons systems programs. Refer to CH 1 Section 3.3 for detailed discussions on organizing an acquisition program.

For an IT program, the hardware/software mix and the degree of customization at minimum will impact how that program is structured and managed — though many other factors ultimately impact these decisions (i.e., funding availability, requirements prioritization, risk, etc.).

In the DoD acquisition context, the terms “Program” and “Increment” refer to the management structure of the acquisition effort. The term “program,” however, is used in confusingly similar ways by the acquisition community as well as other communities within DoD. An “Acquisition Program” is used by the acquisition community to refer to the basic unit of management for an acquisition effort. In the DoD 5000.02 the terms “Acquisition Program” and “Increment” are often used interchangeably.

The basic unit of management for a Weapon System (WS) acquisition is a Program. WS acquisitions are often lengthy endeavors spanning decades. IS or IT acquisitions—in contrast—require a tighter acquisition cycle because technology must be developed or configured and deployed before it becomes obsolete. The pace of development and change in software is fast, and the general expectation is that software acquisitions can and should react at the same speed. Congress has recognized this too, and several statutes now encourage structuring IT acquisitions for shorter, more rapidly deployed Increments.

The Increment, therefore, has quickly become the basic unit for management of an IT acquisition.

The term “Program” in the IT context refers to the summation of a succession of Increments, and is a consolidation of acquisition efforts that is useful for Planning, Programming, Budgeting, and Execution System (PPBE) purposes. An IT “Program” does not have its own APB, rather each Program Increment has its own APB and is a separate acquisition program as defined in DoDD 5000.01 paragraph 3.2 (Para 3.2 – Page 4).

Some additional terms are useful in reference to the software itself. The terms “version,” “release,” and “iteration” all relate to the sequence and importance of a particular software application. For example, the hypothetical Application 2.3.4 is Iteration 4 of Release 3 of Version 2.

The term “version” is regularly used together with a hierarchically structured number such as 2.4.3 to refer to and track the series of improvements or progress of software development. These numbers are assigned in increasing order and correspond to new developments in the software. Logically, the initial
number of a Version should reflect the Increment to which it belongs; Version 3.1.1 should be part of the Increment 3 effort.

**CH 6–3.3 DoD Acquisition Models**

The Department’s six acquisition models are high level processes that encompass the acquisition of a system in the DoD; though not all are used for the acquisition of IT; models 1 and 4 have been omitted from the discussion. Descriptions of all models are available in DoDI 5000.02 paragraph 5.c.(2) (Page 9) as well as CH 1 of the DAG. Table 3 provides descriptions, example and drawbacks of those models that are typically used for acquiring IT in the Department.

**Table 3: Models Used for the Acquisition of IT**

<table>
<thead>
<tr>
<th>Model</th>
<th>Description of Model</th>
<th>Examples</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MODEL 2</strong></td>
<td>Used for complex, usually defense unique software programs that are deployed only</td>
<td>Military unique command and control (C2) systems</td>
<td>Can lead to long waits between deliveries that can cause product obsolescence</td>
</tr>
<tr>
<td>Defense Unique</td>
<td>after several software builds have been completed.</td>
<td>Significant upgrades to the combat systems found on major weapons systems such as surface combatants and tactical aircraft.</td>
<td>cause customer dissatisfaction and push back</td>
</tr>
<tr>
<td>Software Intensive</td>
<td>Program milestones.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Program</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>MODEL 3</strong></td>
<td>Most often referred to as the &quot;Defense Business Systems&quot; Model.</td>
<td>DBSs</td>
<td>Problems in Increments may be difficult to fix in other concurrent Increments.</td>
</tr>
<tr>
<td>Incrementally Deployed</td>
<td>Used for software development programs where the deployment of the full capability</td>
<td>Upgrades to some C2 system software</td>
<td>Concurrent Deliveries can be difficult to manage especially in complex systems.</td>
</tr>
<tr>
<td>Software Intensive</td>
<td>will occur in multiple Increments as new capability is developed and delivered,</td>
<td>Upgrades to weapons systems software</td>
<td></td>
</tr>
<tr>
<td>Program</td>
<td>nominally in 1- to 2-year cycles.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>MODEL 5</strong></td>
<td>It is distinguished from model 2 by the rapid delivery of capability through multiple</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hybrid</td>
<td>Increments.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Program A (Hardware</td>
<td>Each Increment provides part of the overall required program capability.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dominant)</td>
<td>There is some concurrency of development for each Increment.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Can be used for COTS software development with multiple modular capabilities.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Aircraft, ship or land vehicle development where software is a critical component of</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>weapon system delivery.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed
### CH 6–3.4 Common Software Development Methods

The DoD uses many different variations and combinations of software development methods, but they generally fall into three major categories: Waterfall, Incremental and Agile. These development methods are also used for other types of project implementation plans other than SW development. The DoD’s most widely used development method for IT is Incremental, though more and more organizations are working to adopt Agile; or are incorporating principles of agile into their software development practices.

#### CH 6–3.4.1 Waterfall

The Waterfall method is a classical software development method where tasks are arranged to fall sequentially. One phase is completed before the next phase is started. Several software builds are completed before deployment. In its purest form, all requirements are known before IT is developed and the finished product is not delivered until all tasks are completed. For large and complex projects, this can mean that the underlying technology is obsolete before delivery. It also assumes an unrealistic view that organizations are static with the product’s requirements remaining the same throughout the life of the project. If one task is not completed on time, the entire project can be halted. This method provides the greatest risk to user satisfaction; however, it also typically provides the lowest risk to meeting contractual requirements.

#### CH 6–3.4.2 Incremental

The Incremental method has been used to correct some of the problems associated with the Waterfall method. Note that “Spiral” and “Evolutionary Acquisition” are sometimes used synonymously with “Incremental”. These terms actually vary slightly from one another and of the three, the preferred term, as used in the DoDI 5000.02, is Incremental. It has the goal of delivering additional improved capability in block increments over time. This method allows tasks to be developed concurrently. If well managed, this method allows the product to be delivered earlier. In the DoD, you will generally see an initial deployment of 60%-80% of the product delivered; with the remaining capabilities delivered incrementally later.

A variant of Incremental is often used where an Increment is broken down into multiple manageable releases (i.e., Increment 1; Release 1.1; Release 1.2). This may enable both the Functional and the
Program Manager to better manage requirements and deployments into smaller “chunks” of capability, getting capability into users’ hands more quickly.

CH 6–3.4.3 Agile

In 2001 a group of software developers got together to develop a set of best practices for developing software earlier, with greater customer satisfaction, and higher quality. The group developed the Agile Manifesto:

- Individuals and interactions over processes and tools
- Working software over comprehensive documentation
- Customer collaboration over contract negotiation
- Responding to change over following a plan

The manifesto was further elaborated in the Agile Principles.

The best practices established through the Agile Manifesto and Principles are not necessarily new. However, they have been very difficult for the DoD to implement.

In Agile’s purest form, end user(s) should sit with developers in order to make instant decisions on user functionality. High level requirements are initially prioritized and developed quickly by small teams in order to get a working product quickly to the customer. There are several Agile methods have been developed from the Agile Manifesto and Principles including eXtreme Programming (XP), Scrum, and Adaptive Software Development (ASD). An excellent description of the various Agile development methods is provided in a White Paper developed by the Software Engineering Institute titled, “Considerations for using Agile in DoD Acquisition.”

Agile methods are typically used for small, low risk projects. However, some large DBS ERP programs have recently begun to incorporate agile principles to some degree of success, such as using Scrum or Sprints as part of their normal software development practices.

Table 4: A Comparison of Software Development Methods

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
<th>Best Used For</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Waterfall</td>
<td>Uses independent development phases that are completed sequentially</td>
<td>Programs where the requirements are very well understood at the onset of the project</td>
<td>Typically low risk of not meeting contractual requirements if applied correctly</td>
<td>High risk of user dissatisfaction</td>
</tr>
<tr>
<td></td>
<td>Serial, “big-bang” solution with one long cycle times</td>
<td>Functionality to be delivered is mature and static</td>
<td>All functionality is delivered at the same time</td>
<td>Requires a complete set of requirements at the onset</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Best fits with Model 5, though also Model 1 (not described here)</td>
<td>Easiest delivery schedule management</td>
<td>Difficult to incorporate user feedback</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Experimental code or prototypes are discarded after use</td>
</tr>
<tr>
<td>Method</td>
<td>Description</td>
<td>Best Used For</td>
<td>Advantages</td>
<td>Disadvantages</td>
</tr>
<tr>
<td>----------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Incremental | • Development phases can be completed concurrently  
  • Generally 60-80% of product is initially delivered with incremental deliveries delivered later | • Projects where all requirements are not known at beginning of project  
  • Best fits with Models 2, 3, and 6 | • Users can provide feedback earlier  
  • Developers have opportunity to identify potential problems earlier  
  • Does not require a complete set of requirements at onset of project  
  • Overlapping deployments or tasks produce usable functionality earlier | • Schedule with concurrent tasks is difficult to manage  
  • If well managed, project can be delivered earlier  
  • Experimental code or prototypes are discarded after use |
| Agile   | • Customer satisfaction is highest priority  
  • Can be thought of as both a set of software development best practice as well as a software development method  
  • Requirements are prioritized, multiple, rapidly executed  
  • Increments are developed and capabilities are released to the customer as soon as possible  
  • Prototypes may be used as a starting place  
  • It utilizes a modular, open-systems approach  
  • Documentation is kept to an absolute minimum | • Small- to mid-sized applications  
  • Best fits with Models 3, 4, 6 | • Customers get a workable product more quickly  
  • Less documentation, more usable code  
  • Continual involvement of the end user  
  • Developers are able to easily course correct  
  • Scope creep virtually eliminated | • Requires dedicated on site customer collaboration  
  • Difficult to resolve Agile’s lack of documentation required and the DoD’s statutory and regulatory documentation requirements  
  • Difficult to price because all requirements are not scoped at beginning of project |

**CH 6–3.4.4 Approach to IT Acquisition**

The Department’s six acquisition models are high level processes that encompass the acquisition of a system in the DoD. As described in Section 3.3, Models 2, 3, 5, and 6 are the most commonly used for IT acquisition. However, any one of the acquisition models could potentially be tailored and used to acquire IT. The following diagram breaks down a notional version of a DoD acquisition model and explains
various activities that may occur throughout for not only a generic IT acquisition but points out some specialized activities that might occur on a Defense Business System (DBS), for example. These activities will be described in more detail throughout this chapter.

**Figure 2: “Notional” DoD IT Acquisition Model**

**Major IT & DBS Activities**

- **Challenge requirements development outcomes:** (DoD IT acquisition activities) - this includes technical requirements and other targets.
- **Area Knowledge:** (DoD IT acquisition activities) - this includes development of Business, Policy, Planning, and Management. Planning includes: (1) Planning requirements; (2) Functional - Technical requirements; (3) Functional - Non-Technical requirements; (4) Availability target.

**Lifecycle Considerations**

- **Challenge requirements development outcomes:** (DoD IT acquisition activities) - this includes technical requirements and other targets.
- **Area Knowledge:** (DoD IT acquisition activities) - this includes development of Business, Policy, Planning, and Management. Planning includes: (1) Planning requirements; (2) Functional - Technical requirements; (3) Functional - Non-Technical requirements; (4) Availability target.

**CH 6–3.5 DOTMLPF-P Capabilities**

As described in the DoD 5000.02 paragraph 5 b (2), all acquisition programs respond to validated capability requirements. The Department defines capabilities from a holistic, end-to-end standpoint – these are referred to as Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities and Policy (DOTMLPF-P) capabilities. A DOTMLPF-P capability is the ability to perform specific actions that, when taken as a whole, solve a requirement (need, business need, problem, gap, etc.). Capabilities should be forward looking; they describe the business or mission functions that must be executed in the future and they serve as the foundation which the future requirements are derived from, and from which the future program is developed and executed.

In capability analysis, DOTMLPF-P capabilities are always centered on a business or mission function need as opposed to IT or materiel components. The capabilities are also prioritized based on their ability to solve the problem (operational effectiveness) as well as the anticipated benefits of the capability.

The requirements process for most non-IT programs is called the Joint Capabilities Integration and Development System (JCIDS) process. Non-DBS IT programs use the JCIDS IT-Box process, while DBS use the Problem Statement process under the authority of the Deputy Chief Management Officer (DCMO).

Figure 3 illustrates the general interaction between the requirements and acquisition processes. This interaction is also depicted in Figure 2, the Notional DoD IT Acquisition model.
CH 6–3.5.1 JCIDS IT Box

The JCIDS process supports identifying, assessing, validating, and prioritizing joint military capability requirements. The JCIDS IT Box was created to provide agile and responsive capability requirements process to enable rapid development of IT capabilities. Similar to the DBS community, the IS acquisition and programming communities agree that IS development is different from major weapons systems, the processes for which are hardware-focused.

**Figure 4: IT Box Process**
IT Box Applies To | IT Box Does Not Apply To
--- | ---
- Information Systems (IS) with software development only
- Includes integration of COTS hardware
- Program costs that exceed $15 million
- Defense Business Systems (DBS)
- Systems that are an integral part of a weapon or weapon system
- IS with a developmental cost less than $15 million

The Information System Initial Capabilities Document (IS-ICD) and the IS-Capabilities Development Document (IS-CDD) are used in implementation of the IT Box. These are variants of the standard ICD and CDD used in the JCIDS process and are designed to focus on facilitating more efficient and timely software development efforts. The major difference between the IS-ICD and the IS-CDD is that capabilities outlined get refined and presented as Key Performance Parameters (KPPs), Key System Attributes (KSAs) with specific threshold requirements and objective targets. CDDs are not required as successor documents for non-MDAP IS-ICDs and CPDs are not required as successor documents for IS-CDDs. CH 7 also discusses JCIDS documents from an intel perspective.

Detailed Guidance for the Information System ICD (IS-ICD) and the IS-CDD are provided in the JCIDS Manual. An IT Box Primer has also been developed by DAU.

Detailed guidance for both the IS-ICD and IS-CDD are provided in the JCIDS Manual which includes examples of potential IS ICD/CDD follow-on documents such as the following:

- Requirements Definition Package (RDP) – identifies KPPs and nonmaterial changes
- Capability Drop (CD) – lower level document that specifies the characteristics of a “widget” or “app” for partial deployment of the system

As the IS-ICD and IS-CDD only streamline the applicable requirements processes, the Sponsor must still ensure compliance with acquisition policy and processes in DoDI 5000.02.

**CH 6–3.5.2 Defense Business Systems**

Defense Business Systems (DBS) support DoD business activities such as acquisition, financial management, contracting, logistics, strategic planning and budgeting, installations and environment, and human resource management. DBS follow a process governed by Title 10, U.S.C. section 2222 and the Defense Business Council (DBC) and have unique processes and procedures in both the requirements and acquisition aspects of the DoD Acquisition lifecycle. They do not follow the IT-Box and do not generally utilize IT-Box or traditional JCIDS process documentation.

Additional information about the DBC can be accessed from DCMO’s DBC webpage. The DBC is the governing body who oversees defense business operations on behalf of the Secretary under the authority of Title 10, U.S.C. section 2222 and the DBC Charter.

The DBC serves as the:

- Principal governance body for vetting issues related to management, improvement of defense business operations; and other issues to include performance management, pursuant to the Government Performance and Results Modernization Act (GPRMA) of 2010 (Public Law 111-352).
- Department’s Investment Review Board (IRB) for business systems, pursuant to Title 10, U.S.C. section 2222.

The DBC is co-chaired by the Deputy Chief Management Officer (DCMO) and the DoD Chief Information Officer (CIO).

Defense Business System (DBS) capability requirements are defined beginning with the Problem Statement and other supporting documentation such as a System Requirements Document (SRD) or Capabilities Requirements Document (CRD), though the methods through which more detailed
requirements are documented are not dictated by policy. Capability requirements are further defined throughout the lifecycle of the system. Configuration Control Boards (CCBs) are most often used to determine capability requirement veracity and priority.

DBS do not use the JCIDS process for defining requirements, generally, unless the requirement is deemed joint interest. At that point, the Joint Staff will provide guidance for any additional requirements or documentation that will be needed.

**CH 6–3.5.2.1 Problem Statements**

A Problem Statement identifies a business need and the Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities and Policy (DOTMLPF-P) capabilities required to solve it. A Problem Statement is required for all expected DBS investments expected to cost $1M or more over the FYDP. Recent changes implemented by the FY2016 National Defense Authorization Act (NDAA) will affect not only the threshold for the Problem Statement Process but will likely drive changes to the overall process and templates used for it. Revised guidance from the Office of the DCMO is forthcoming – current and revised guidance is located on the DCMO website.

A Problem Statement should not be an IT solutions document. Rather, it should clearly define a need, why it exists, the context in which it exists, and the intended outcome that is desired from solving the need expressed as a comprehensive DOTMLPF-P capability. In addition, the Problem Statement includes measurable business outcomes, a rough order of magnitude cost estimate and projected/anticipated financial return measures such as net present value, payback or return on investment.

The Problem Statement is refined over time (i.e., decomposed into greater detail as more information is known). However, it is often approved only once unless a substantive scope change or fundamental change to the business need occurs. The Problem Statement must be validated by the prior to a Materiel Development Decision (MDD) or equivalent. It also serves as an input to the acquisition process and to the acquisition strategy, as well as any more detailed requirements planning.

Generally, all DBS follow processes defined by the DCMO for capability requirements review. However, the Joint Requirements Oversight Council (JROC) has the ability to review Problem Statements to determine if JROC interest exists. At that time, the JROC (or the applicable Functional Capabilities Board [FCB]) may levy additional requirements on the DBS for requirements review.

**CH 6–3.5.2.2 Authority to Proceed (ATP) Decisions**

DBS more and more frequently use event-based decision points called ATPs. An ATP is a method of tailoring for DBS in order to achieve more efficient and effective capability delivery, wherein regulatory requirements are “tailored in” rather than “tailored out”. ATPs may be used to authorize entry into a new program phase, denote the authorization of program activity, or in lieu of a standard acquisition milestone such as an A or a B. There are three critical things to keep in mind when using ATPs:

- Use of an ATP should be based on the specific DBS product and overall approach to DOTMLPF-P capability delivery.
- The Program Manager should propose usage of ATPs and associated documentation requirements to the MDA as early as possible and document the MDA’s tailored approach in the program acquisition strategy.
- Statutory requirements normally aligned to acquisition milestones must be completed and aligned with an analogous ATP; statutory requirements cannot be waived unless the statute permits.

**CH 6–3.5.3 Business Process Reengineering (BPR)**

Modifying the core code of a Commercial-Off-The-Shelf (COTS) product should be avoided. Importantly, business process reengineering is a function applicable to all IT that involves a process as its backbone to operate. BPR is most commonly thought of, however, as a companion activity to business system implementation. For DBS under Title 10 U.S.C. section 2222 it is directed that “defense business processes are reviewed, and as appropriate revised, through business process reengineering to match best commercial practices, to the maximum extent practicable, so as to minimize customization of commercial business systems”.
Adhering to the processes in a COTS product as much as possible is an industry best practice. A 2015 report by Panorama Consulting found that of the 562 companies they surveyed:

- The majority (66%) did little to no customization (defined as modifying one-quarter or less of the solution).
- 34% did “significant” (22%), “extreme” (7%), or “complete” (5%) customization to their ERP implementation.

In industry, customization is most often focused on processes that will give a company competitive advantage or make them unique – however; since the federal government is not profit-driven and rather is being mandated by Congress to specifically not customize its products, the push should be to utilize BPR and to adhere to the out of the box products as much as possible. Functional Sponsors and Program Managers should try to find ways to modify existing business processes rather than customizing commercial software products to meet their needs. Discussions on common standards (Section 3.7) and requirements and configuration management (Section 3.5.5) are important to being successful in this area.

While it is possible to add code in the form of Reports (R), Interfaces (I), Conversions (C), Enhancements (E), Forms (F) and Workflows (W) (RICE-FW), this practice significantly increases program costs and should be minimized as much as possible through BPR. In many cases there will only be a few instances where BPR is not possible. For example, due to policy or law, it may be necessary to build or acquire needed reports, interfaces, conversions, and extensions. In these cases, adding to the product must be done under strong configuration control.

The Functional Sponsor, representing the needs of the user, leads the BPR effort. BPR may include eliminating non-value added processes, consolidating separate functional tasks into end-to-end cross-functional processes, and integrating business functions as much as possible to improve business operations and to achieve the desired outcome(s). BPR is a continuous process and requires a rethinking of why the “As-Is” process came to be and how it can be improved to achieve efficiencies.

Ideally BPR will begin prior to the start of the Acquisition process to understand the picture of “what good looks like”. However, BPR truly cannot be completed until a solution is selected to understand the underlying business processes of the product.

**Major duties and responsibilities of BPR stakeholders:**

- The Functional Sponsor (or Sponsor), informed by input from the corresponding DoD Military Component, is responsible for BPR.
- The PM is responsible for analyzing and considering the results of the BPR and using the goals of the reengineered process to shape the program.
- Technical SMEs (including test and engineering), to understand the impact of process changes vs. technical changes
- Cost SMEs, to understand the cost impacts of process changes vs. technical changes

**CH 6–3.5.4 Developing Relevant Outcomes**

Successful capability delivery in IT programs relies upon the ability to track progress toward completion. Generally, Performance Measures/Attributes are used to determine the degree to which a DOTMLPF-P capability has been successfully implemented. Measures and Attributes are tied to each Capability in order to answer the question: how will we know if this Capability has been fulfilled? The Performance Measures are defined at a mission or business level and can be broken down into process or system metrics later in the transformation effort. Outcomes define “what good looks like” to indicate when success has been achieved at varying levels (strategic, business, program, KPPs, KSAs, etc.) – and, to indicate when failure may be on the horizon.

Performance measures identify the performance-based metrics that provide visibility to the outcomes progress towards completion. IT programs should initiate a top-down decomposition process of outcomes
and performance measures development, where high-level outcomes are developed early on and then decomposed further into business and program outcomes as more detail is learned throughout.

Any outcome should explicitly state the business value of the resources to be invested and to allow leadership to prioritize and weigh investments. The outcome provides strategic alignment and clear criterion against which to evaluate potential approaches. It always starts with the desired result and is used to focus behaviors and results by answering the “what’s in it for me?” question. Corresponding measures must be specific, actionable, measurable, relevant, and timely operational capabilities that can be achieved against their corresponding outcomes.

It is important to note that the Functional Sponsor (who represents the needs of the user[s] that originally identified the problem, need, or requirement) is ultimately responsible for declaring whether the needed capability has been delivered.

Integrated teams should develop measures and metrics – while the exercise may be led by a Functional Sponsor or representative, it requires involvement from the Program Manager or key representatives from the program office, as well as SMEs from the test and engineering communities to ensure that measures are realistic, relevant, and testable from the beginning.

CH 6–3.5.5 Requirements Management

Documenting and managing requirements is one of the biggest challenges in DoD IT systems, and is critical to ensure effective delivery of a comprehensive DOTMLPF-P capability. For example: A 2009 GAO audit found that DoD and service officials responsible for conducting AoA’s indicated that often proposed capability requirements are so specific that they effectively eliminate all but the service sponsor’s preferred concepts instead of considering other alternatives (GAO-09-655, September 2009).

The process of requirements and configuration management is described in CH3, Systems Engineering and also in DoDI 5000.02 Encl. 3 Section 8 of DoDI 5000.02. The bottom line is that ensuring strong requirements and configuration management processes will ensure traceability and insight into all levels of development and design of the DOTMLPF-P solution. It is critical to establish and maintain consistency of a system’s functional, performance, and physical attributes with its requirements, design, and operational information throughout a system’s life cycle.

Effective control processes will allow a PM to better manage cost, schedule, and performance; and enable the PM to deliver a product that the Functional customer had envisioned:

- Configuration Control Boards (CCBs)
  - The use of CCBs is one of the most common (and effective) ways to control and manage requirements on IT programs. CCBs are most commonly partnerships between the functional and programmatic communities, involving tradeoffs of software requirements – depending on what level the CCB is held at in the organization. They may be referred to as Enterprise (or Executive) CCBs, Software CCBs, Requirements CCBs, or by other nomenclatures.

- Baseline Management
  - Depending on the type of IT implementation, many programs manage the implementation of the software baseline (and changes to it) separately from the modernization program. This can offer both challenges and benefits, but managing separately can become unwieldy on a large program if the efforts are not in sync with one another.

- Tools
  - Many DoD IT programs, most often due to the volume of requirements they must contend with, use automated tools to manage different parts of the requirements process – and some are customized for the type of software development process that is being followed. The scope of tools available include: Issue Management, Agile, Project Management, Product Management, Requirements Development, Requirements Management, Visual Modeling, Testing, User Interface/User Experience (UI/UX) Mockup, etc.
CH 6–3.6 Managing IT Program Investments

The overarching Planning, Programming, Budgeting, and Execution process is described in CH 1 Section 3.2.2 and Cost Estimation in CH 1 Section 3.4.3.5. Defense Budget Materials are available on the DoD Comptroller’s website and are updated every Fiscal Year. Finally, DAU offers a continuous learning module, CLB 023 Software Cost Estimating. Annual IT Budget Submission guidance is published by the DoD CIO to adjust the submission process outlined in the FMR to ensure currency with OMB guidance. Contact DCIO-R&A or your Component budget office for the most current guidance.

More specifically, there are two major budget submission requirements for DoD IT investments: IT Budget Estimate Submission (BES) and the Congressional Justification submission or President's Budget (PB) Request. Instructions for submitting IT specific budgets can be found in DoD 7000.14-R Financial Management Regulation Volume 2B, Chapter 18 Information Technology (Including Cyberspace Operations) dated September 2015.

DoD utilizes several systems to capture and maintain IT investment information including Department of Defense Information Technology Investment Portal (DITIP) and the Select & Native Programming Data Input System for Information Technology (SNaP-IT).

During the first phase in the annual budget cycle, the Office of the Director, Cost Assessment and Program Evaluation (D, CAPE) and the Office of the Under Secretary of Defense (Comptroller) (USD(C)) are responsible for conducting an annual Program Budget Review PBR on all DoD resources and require a data submission from all DoD Components.

Components are also required to submit supplemental PBR data on their Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) programs. This supplemental submission of MDAP and MAIS data supports ongoing OUSD(AT&L) data transparency and data alignment efforts initially directed in the Fiscal Year 2011 Integrated Program Review Resource Management Directive 700 study.

Data submission is required for all current MDAPs and MAIS programs, as well as acquisition program concepts and Unbaselined MAIS programs that will achieve Milestone B prior to the end of the calendar year, or have been certified under the provisions of section 2366a of title 10 United States Code. The MDAP and MAIS program data must include all acquisition costs (RDT&E, Procurement, MILCON, Acquisition O&M, Working Capital Funds, or Other Financing with an explanation) and MDAP quantities (RDT&E and Procurement) for the full acquisition cycle of each MDAP and each MAIS program (by fiscal year and funding appropriation). For MAIS programs, the total life-cycle cost is the development cost plus 10 years of Operation and Support (O&S) costs following Full Deployment declaration. For MDAP programs, the full acquisition lifecycle and associated funding is defined by the D, CAPE and USD(C) PBR Submission Guidance.

All MDAPs and MAIS programs submit annual PBR data that has been coordinated with and approved by the appropriate Component Acquisition Executive (CAE) into their Component's acquisition information system. For efficient information sharing, the CAE systems publish the data to Acquisition Visibility (AV) using the Defense Acquisition Management Information Retrieval (DAMIR) system Web Services. Components without access to one of the Component acquisition information systems use the DAMIR "Create or Edit a Budget Report" module. Notwithstanding the method of transmission, exposure, or publication, the CAE-approved PBR data is be available for consumption by AV and AV subscribers as determined by annual guidance.

CH 6–3.6.1 Federal IT Dashboard

The Federal IT Dashboard (ITDB) displays general information on over 7,000 Federal IT investments and detailed data for over 700 "major" investments. DoD’s IT investments on the Federal IT Dashboard span the investment lifecycle (planning and budgeting, acquisition, management in-use). A general overview and tutorial of the Federal IT Dashboard can be accessed here. The DoD CIO ratings process is conducted semiannually and was designed in accordance with Office of Management and Budget (OMB) and internal DoD policies, processes, and procedures.
The Federal ITDB has high visibility with GAO, OMB, and now even Congress, who all use it as a tool to identify troubled investments. The Federal Information Technology Acquisition Reform Act (FITARA) now requires the DoD CIO to review any DoD investment on the ITDB that receives a high risk rating for four consecutive quarters and provide a report to relevant House and Senate committees, in addition to OMB.

The DoD CIO publishes guidance on how to assess investments that must be reported on the Federal IT dashboard and utilizes a CIO Ratings Recommendations submission page (CAC-enabled), which contains the latest reference documents, approved ratings, stakeholder ratings recommendations, and POCs for completing the ratings process. Guidance is provided in the "Department of Defense Chief Information Officer (DoD CIO) Ratings Process for the Federal Information Technology (IT) Dashboard," dated March 25, 2014 and available within the above linked site.

**CH 6–3.6.2 IT Budget Estimate Submission (BES)**

Guidance and formats for the preparation and submission of the Information Technology Budget Estimate Submission (BES) to the DoD CIO are provided in DITIP and through SNaP-IT.

**CH 6–3.6.3 President's Budget (PB) Request**

The President's budget request for the DoD is submitted to Congress by the President. All DoD Components that require funding for IT programs and/or Cyberspace operations submit budget requests that are authorized by the DoD Component, OSD, the Office of Management and Budget (OMB), the President, and ultimately by Congress. Budget requests are prioritized based on the mission objectives of the Component, DoD and the President. General guidance for budget request submission requirements is presented in Volume 2A, Chapter 1 of the DoD Financial Management Regulation (FMR) and in the OSD Program/Budget guidance memos.

**CH 6–3.6.4 MAIS Annual Report (MAR)**

**Title 10 U.S.C. section 2445b** requires that the Secretary of Defense submit, to the Congress, annual reports on all MAIS, Unbaselined MAIS and pre-MAIS acquisition programs. This annual report, known as the MAIS Annual Report (MAR), is also a budget exhibit. The MAR is submitted through the Defense Acquisition Management Information Retrieval (DAMIR) system. MARs are delivered to Congress within 45 days after the President’s Budget, as directed by statute.

**CH 6–3.6.4.1 OMB Policy**

OMB Circular A-11 provides guidance to Federal programs on how to prepare and submit materials required for OMB and Presidential review of agency budget requests. The guide to OMB Circular Number A–11 provides a description of the contents of the Circular. Section 25.6 of the Circular provides a table with the required contents of the Budget Request to be submitted to OMB.

**Section 53 of Circular A-11** provides guidance pertaining to IT and E-Government. Specifically it provides instructions for submitting an Agency’s IT Portfolio Summary (formally known as Exhibit 53A), an Agency’s IT Security Portfolio (formally known as 53B) and an Agency’s Cloud Spending Summary (formally known as 53C).

The policy and specific instructions on managing Federal information resources are provided in OMB Circular A-130, "Management of Federal Information Resources." The policies in the Circular apply to the information activities of all agencies of the executive branch of the Federal government. The Department of Defense Information Technology Information Portal (DITIP) and/or Select and Native Programming – Information Technology (SNaP-IT) systems are used to gather information requested by OMB.

**CH 6–3.6.4.2 IT Business Case**

The IT Business Case, formerly known as the Exhibit 300, pertains to reporting requirements for Section 55 of OMB Circular A–11. The Major IT Business Case Exhibit (see page 40 of FY 2019 IT Budget – Capital Planning Guidance) (formally known as Exhibit 300A) and the Major IT Business Case Detail Exhibit (see page 34 of FY 2019 IT Budget – Capital Planning Guidance) (formally known as Exhibit 300B) are companion pieces an Agency’s IT Portfolio Summary, IT Security Portfolio and Cloud Spending Summary. These Exhibits, together with the agency’s Enterprise Architecture program, define how to
manage the IT Capital Planning and Control Process. The IT Portfolio Summary is a tool for reporting the funding of the portfolio of all IT investments within a Department while the Major IT Business Case Exhibit is a tool for detailed justifications of major “IT Investments”. The Major IT Business Case Detail Exhibit is for the management of the execution of those investments through their project life cycle and into their useful life in production.

In a January 8, 2016 memorandum the Director, Acquisition Resources and Analysis and Deputy CIO for Resources and Analysis wrote that “starting with the FY 2017 President’s Budget (PB) submission, the Department will singularly report to Congress and the Office of Management and Budget (OMB) utilizing the annual (MAIS Annual Report) and (Selected Acquisition Report) submissions”, to eliminate duplicate reporting in the former Ex. 300. It is important to note that this is a rapidly changing process in the Department and applies only to active MDAP and MAIS programs currently using the MAR or SAR to accomplish the business case requirement. It is very likely that updated guidance on the business case requirement will be issued imminently. For example, beginning with the FY2018 PB, the Department is planning to utilize similar MAR-like data reporting and processes for all Major IT Investments – even if they currently do not report as part of a MAR or SAR process.

**CH 6–3.6.5 Affordability**
The purpose of conducting an Affordability Analysis is to avoid starting or continuing programs that cannot be produced and supported utilizing future budgets. Affordability is relatively straightforward when procuring tanks; however, it can be difficult to determine for some IT investments such as IT Services where there are no specific “units”.

The best opportunity for determining affordability is through tailoring capability requirements before and during the development of an Analysis of Alternatives (AoA). Components should incorporate estimated funding streams for future programs within their affordability analyses at the earliest conceptual point and specify those estimates at the MDD and beyond to inform system design and alternative selection.

Prior to MS B (or the equivalent ATP), affordability goals are considered targets and are used to help scope the AoA and other required analyses in order to achieve an affordable program to be put on contract at RFP release and to be baselined at MS B. Once requirements and the product definition are firm, affordability caps are established to provide fixed cost requirements that are functionally equivalent to Key Performance Parameters (KPPs).

Additional policy regarding conducting affordability analysis is located in DoDI 5000.02 (Encl. 8) Enclosure 8 of DoDI 5000.02 and DoDI 5000.02 (Encl. 10 — sec 2) Enclosure 10 Section 2 of DoDI 5000.02 (Encl. 10 — sec 2).

**CH 6–3.6.6 Lifecycle Cost Estimating for IT**
Developing a well thought out Lifecycle Cost Estimate (LCCE) with costs from inception to retirement is crucial for the following:

- Establishing fiscal feasibility of the program
- Informing Analyses of Alternatives (AoAs)
- Guiding capability requirements and engineering tradeoffs
- Setting realistic program baselines to control life-cycle costs, and
- Instill more cost-conscious management in the DoD.

Life-Cycle Cost (LCC) estimating represents the total cost to the Government for an IS, weapon system, program and/or investment over its full life. It includes all developmental costs, procurement costs, MILCON costs, operations and support costs, and disposal costs. LCC encompasses direct and indirect initial costs plus any periodic or continuing sustainment costs, and all contract and in-house costs, in all cost categories and all related appropriations/funds.

LCC may be broken down to describe the cost of delivering a certain capability or useful segment of an IT investment. LCC normally includes 10 years of sustainment funding following Full Operational Capability (FOC) or Full Deployment for Automated Information Systems. For investments with no known end date that are beyond FOC, LCC estimate should include 10 years of sustainment.
The Director of Cost Assessment and Program Evaluation (DCAPE) provides policies and procedures for developing LCCEs for all DoD acquisition programs. DCAPE also reviews cost estimates and cost analyses conducted in connection with Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) programs.

The DCAPE also conducts Independent Cost Estimates (ICE) and cost analyses for MAIS (if directed by the MDA, or if a program is in a critical change – otherwise an ICE is typically not required) and MDAP programs. The documentation of each MDAP or MAIS program cost estimate prepared by DCAPE and/or Service or Agency includes the elements of program cost risk identified and accounted for, how they were, evaluated and possible mitigation measures.

The DCAPE requires use of a Cost Analysis Requirements Description (CARD). The CARD is a complete description of the system at a level of detail appropriate for calculating costs. DCAPE provides CARD development guidance tailored to the specific review being conducted and the type of system being developed. However, all CARDS, no matter how tailored, will provide a program description that includes a summary of the acquisition approach, expected constraints, system characteristics, quantities, operational factors, operational support strategy, preliminary schedules, test programs, technology maturation and risk reduction plans, and appropriate system analogs. Additional content may be required as requested by DCAPE.

Should the contractor proposed solutions entering the Technology Maturation and Risk Reduction Phase differ significantly from the design reflected in the Milestone A CARD, the Program Manager will report any differences that might alter the basis for the MDA’s Milestone A decision to DCAPE and the MDA. The MDA will determine whether an additional review is required prior to contract award.

At the Development RFP Release Decision Point, the program described in the final CARD will reflect the Program Manager’s and PEO’s best estimate of the materiel solution that will be pursued following Milestone B. The final CARD is updated to reflect all new program information prior to Milestone B.

For DBSs, a Cost Element Structure is required when developing a Business Case. An example of commonly used elements is provided in the DoD Enterprise IT Business Case Analysis Template Appendix B. The Cost Element Structure is the most critical element of the BCA process to ensure consistent, comparable cost estimates on IT.

DoD Components develop a DoD Component Cost Estimate that covers the entire life cycle of the program for all MAIS programs at any time an Economic Analysis is due.

CH 6-3.6.6.1 Should-Cost and Will-Cost

The concept of “should-cost” is driven by the DoD culture of cost-consciousness. It is focused on controlling the cost of the actual work that we are doing and expect to do and to identify and eliminate inefficient and non-productive tasks from our programs. Should-cost is a tool to manage all costs throughout the lifecycle, and it operates in parallel with the effort to constrain requirements in order to costs all the way through to sustainment of the capability. In particular, should-cost estimates inform negotiations with industry over contract costs and incentives. The should-cost approach challenges us to do our best to find specific ways to beat the Independent Cost Estimate (ICE) or Program Estimate (which should already reflect the affordability requirements) and other cost projections funded in budgets (i.e., “will-cost”), when we find sensible opportunities to do so. For example, should-cost does not mean trading away the long-term value of sound design practices and disciplined engineering management for short-term gain.

In 2011, the USD(AT&L) and the Comptroller signed out a memo containing the “ingredients” to should-cost management. Another excellent resource is the April 2014 issue of the Defense Acquisition Research Journal examined how programs have implemented should-cost, the types of savings identified.
and realized, and best practices and lessons learned that might be adopted by other programs in the Department.

Should-cost is reported through the DAES review process. For additional information on should-cost and will-cost, visit CH 1 Section 4.2.17.

**CH 6–3.6.7 Program Funding Chart**
The program funding chart is often referred to as the "Spruill Chart". The purpose of the Program Funding Chart is to capture the primary acquisition and sustainment program budgets relative to the previous President’s Budget and latest estimate of funds required to execute the program. Instructions and links to the Spruill Chart are available [here](#) and are CAC-enabled. The template is updated as Programming, Planning, Budgeting, and Execution System (PFBE) events occur. The Spruill Chart features prominently throughout the DAB process.

The basic instructions for the Spruill Chart are to report all RDT&E, Procurement and MILCON investments supporting the baselined acquisition program, consistent with the Selected Acquisition Report (if applicable). Report all weapon system O&M associated with the program, consistent with the Operating and Support estimates reported in the SAR (if applicable). Other appropriations supporting O&S are not reported.

**CH 6–3.6.8 IT Portfolio Management**
Portfolios can be based on mission areas or commodity types, and will define a collection of products or capabilities that can be managed together for investment analysis and oversight purposes. Components will normally make tradeoffs within portfolios, but if necessary, can and should make tradeoffs across portfolios to provide adequate resources for high-priority programs.

Component level affordability analysis examines all programs and portfolios together, extending over enough years to reveal the life-cycle cost and inventory implications of planned program for the Component. The same analysis is used as individual programs come up for review. Nominally, affordability analysis covers 30 to 40 years into the future.

Authority for portfolio management is found in many locations. For example:

- DoDI 5000.02
- DoDD 8115.01 "Information Technology Portfolio Management"
- DoDI 8115.02 "Information Technology Portfolio Management Implementation"
- DoDD 7045.28 "Capability Portfolio Management"

Guidance or best practices on how to conduct portfolio management is more difficult to come by.

- For DBS specifically: [Guidance for Review and Certification of Defense Business Systems version 4.0, April 2017](#)
- GAO 15-466, "Opportunities Exist to Improve the Department of Defense’s Portfolio Management"

**CH 6–3.6.8.1 Defense Business Systems Investment Review (Certification)**
Certification of investments are required for covered defense business systems (i.e., those DBSs with funding >$1M over the period of the current Future Years Defense Program (FYDP)). All appropriations require certification. In addition, all funding including funds from another DoD Component must be certified. These rules have changed with the FY2016 NDAA and this guidance will be updated accordingly when the DCMO introduces updated policy.

As part of the DBS certification process, DoD Components (e.g., MILDEPS and Defense Agencies) annually develop Organizational Execution Plans (OEPs). Each OEP is comprised of three elements: the Portfolio Certification Request, the OEP briefing, and views of authoritative data from [DoD Information Technology Portfolio Repository (DITPR)](#) and [Select & Native Programming Data Input System for Information Technology (SNaP-IT)](#). DoD Defense Business Council (DBC) members assess Component
OEPs and provide recommendations to the Chair on certification of funds. The DCMO approves OEP certifications and records the outcomes in investment decision memoranda (IDMs).


CH 6–3.6.8.1.1 Integrated Business Framework
The Integrated Business Framework provides the overarching structure used to govern and manage the Department’s business operations from the creation of aligned business strategies and investment plans, to the measurement of outcomes. A description of the framework is provided on Page 5 of the DCMO’s Guidance for Review and Certification of Defense Business Systems, version 4.0, April 2017. The framework is also designed to facilitate a cross-functional, enterprise-wide view for the governance of portfolios of DBS investments over the FYDP for review and certification. The DoD's Strategic Management Plan (SMP) is an enterprise plan for improving DoD's business operations. The Department is currently transitioning toward incorporating the business strategy into an Agency Strategic Plan (ASP) that will provide a more comprehensive plan and measures.

CH 6–3.6.8.2 Clinger-Cohen Act
The Clinger-Cohen Act, or Subtitle III of Title 40 of the United States Code Title 40 U.S.C. Subtitle III (formerly known as Division E of the Clinger-Cohen Act (CCA) (hereinafter referred to as “Title 40/CCA”) applies to all IT investments, including National Security Systems (NSS). Title 40/CCA requires Federal agencies to focus more on the results achieved through its IT investments, while streamlining the Federal IT procurement process. Specifically, this Act introduces much more rigor and structure into how agencies approach the selection and management of IT projects.

Title 40/CCA generated a number of significant changes in the roles and responsibilities of various Federal agencies in managing the acquisition of IT. It elevated oversight responsibility to the Director of the Office of Management and Budget (OMB) and established and gave oversight responsibilities to the departmental Chief Information Officer (CIO). Also, under this Act, the head of each agency is required to implement a process for maximizing the value and assessing and managing the risks of the agency's IT acquisitions.

In DoD, the DoD CIO has the primary responsibility of providing management and oversight of all Department IT to ensure the Department's IT systems are interoperable, secure, properly justified, and contribute to mission goals.

The basic requirements of the Title 40/CCA, relating to DoD's acquisition process, have been institutionalized in DoD Instruction 5000.02, in particular, Enclosure 11 (IT Considerations). The requirements delineated in this section must also be considered and applied to all IT investments, regardless of acquisition category, and tailored commensurate to size, complexity, scope, and risk levels.

Figure 5: Title 40 – Clinger Cohen Act Compliance

Field Code Changed
Field Code Changed
Field Code Changed
Field Code Changed
Field Code Changed
PMs, program sponsors/domain owners, members of the joint staff, and DoD Component CIO responsibilities are further explained and detailed in the IT Community of Practice Knowledge Center, which also contains a vast array of information pertinent to specific aspects of Title 40/CCA compliance.

A comprehensive compilation of Federal laws, OMB and Budget circulars, DoD directives and instructions, and OSD policy memorandums, relevant to all aspects of Title 40/CCA compliance, is available in the CCA Policy Folder of the Acquisition Community Connection. The Title 40/CCA Compliance Table details actions required to comply with Title 40/CCA regulatory requirements, mandatory DoD policy, and the applicable program documentation that can be used to fulfill the requirement.

The requirements in this table must be satisfied before Milestone approval of any Acquisition Category (ACAT) I (i.e., Major Defense Acquisition Program (MDAP)) and ACAT IA (i.e., MAIS Program) and prior to the award of any contract for the acquisition of a Mission-Critical or Mission-Essential IT system, at any level.

The requirements delineated in this table must also be considered and applied to all IT investments, regardless of acquisition category, and tailored commensurate to size, complexity, scope, and risk levels.

**CH 6–3.6.9 Contracting - Special Circumstances and Best Practices**

Fundamentally, there is no one “best fit” type of contract for the acquisition of information technology. Many program offices have found that having a contracting officer integrated into the program planning activities up-front to gain subject matter expertise into the IT capability enables more appropriate contracting vehicles to be applied.

When acquiring IT and developing requests for proposals (RFPs) and contract statements of work (SOWs), they should be reviewed as part of the acquisition process to ensure that IT standards established in a program’s requirements document are translated into clear contractual requirements.

Various methodologies, toolsets, and information repositories have been developed to assist the Program Manager (PM) in the implementation of COTS software-based programs. The remainder of this section provides the PM descriptions of best practices, available tools and methods, and critical success factors for use in the acquisition of commercially-based solutions.
CH 6–3.6.9.1 Enterprise Software Initiative

The DoD Enterprise Software Initiative (DoD ESI) is a joint, Chief Information Officer (CIO)-sponsored project designed to: "Lead in the establishment and management of enterprise COTS information technology (IT) agreements, assets, and policies for the purpose of lowering total cost of ownership across the DoD, Coast Guard and Intelligence communities." DoD ESI is a key advisor to the DoD Strategic Sourcing Directors Board. With active working members from OSD, Department of the Army, Department of the Navy, Department of the Air Force, Defense Logistics Agency, Defense Information Systems Agency, National Geospatial-Intelligence Agency, Defense Intelligence Agency, Director of National Intelligence, and Defense Finance and Accounting Service, the DoD ESI team collaborates to create Enterprise Software Agreements (ESA) for use by DoD, the Intelligence Community, and U.S. Coast Guard IT buyers. ESA negotiations and management activities are performed by IT acquisition professionals within participating DoD Components, who are designated ESI "Software Product Managers (SPM)." SPMs are supported by experienced IT contracting experts.

The DoD ESI can use the Defense Working Capital Fund to provide "up-front money" for initial wholesale software buys and multi-year financing for DoD customers. This funding process assures maximum leverage of the combined buying power of the Department of Defense, producing large software cost discounts.

On-line resources include the DoD ESI website listing general products, services and procedures the Defense Federal Acquisition Regulation Supplement Subpart 208.74; and the DoDI 5000.02 (Enclosure 11, Sec. 10).

CH 6–3.6.9.2 Defense Federal Acquisition Regulations

The Defense Federal Acquisition Regulations (DFARs) contains contractual requirements for IT. Some of the subsections of interest are subpart 239.71 regarding security and privacy for computer systems, subpart 208.74 on enterprise software agreements and subpart 227.72 for policy on the acquisition of commercial computer software and commercial computer software documentation.

CH 6–3.6.9.3 Defense Information Systems Agency (DISA) Support

Purchasing telecommunications and IT products and services for the military is one of DISA's key roles within the DoD. The DISA Contracts Guide (CAC Only) is provided by Defense Information Technology Contracting Organization (DITCO); it contains a list of Premier Contracts as well as ordering instructions. In addition:

- DISA provides Enterprise Acquisition Services (EAS) for purchasing telecommunications and information technology (IT) products and services from the worldwide commercial sector to meet Department of Defense (DoD) and authorized non-defense customers' needs. Services include acquisition planning, procurement, tariff surveillance, cost and price analyses, and contract administration. DISA is the mandated single source for procuring DoD long haul telecommunications requirements.
- DISA establishes large contract vehicles available to DoD for essential IT services such as engineering, hardware, equipment and maintenance, integration and support, information security, computer technology, satellite bandwidth, and Defense Information System Network (DISN) access.

CH 6–3.6.9.4 Strategic Sourcing

Strategic Sourcing is about buying smartly and collaboratively in an effort to reduce costs and maximize the use of available funds. While this concept is most often thought of in the context of supply chain management, it has strong applicability to information technology in terms of buying bulk software, licenses, and / or services. Resources for Strategic Sourcing assistance include:

- In an effort to enhance collaboration and integration, the OSD Office of Defense Procurement and Acquisition Policy (DPAP) provides multiple resources for Strategic Sourcing opportunities and best practices and sits on the government-wide Strategic Sourcing Leadership Council (SSLC), whose objective is to lead the government's efforts to increase the use of government-wide management and sourcing of goods and services.
DPAP also has a DoD-Wide Strategic Sourcing (DWSS) CONOPS available to explain how to use the DWSS program.

Finally, the DAU Acquisition Community Connection has a Community of Practice for Strategic Sourcing available with many best practices.

CH 6–3.6.9.5 Data Rights

Data Rights is a shorthand way to refer to the Government’s license rights in major categories of valuable intellectual property, and it factors critically into how a capability is contracted for and how data is managed for the life of a program. Data Rights are also discussed in CH 4 Section 3.3.1.11.

Data Rights for technical data and computer software fall into eight categories:

- **Unlimited Rights.** Developed exclusively at Government expense, and certain types of data (e.g., Form, Fit, and Function data [FFF]; Operation, Maintenance, Installation, and Training [OMIT]), these rights involve the right to use, modify, reproduce, display, release, or disclose technical data in whole or in part, in any manner, and for any purpose whatsoever, and to have or authorize others to do so.

- **Government Purpose Rights.** This right involves the right to use, duplicate, or disclose technical data for Government purposes only, and to have or permit others to do so for Government purposes only. Government purposes include competitive procurement, but do not include the right to permit others to use the data for commercial purposes.

- **Limited Rights.** A limited rights agreement permits the Government to use proprietary technical data in whole or in part. It also means that the Government has to obtain the expressed permission of the party providing the technical data to release it, or disclose it, outside the Government.

- **Restricted Rights.** Developed exclusively at private expense

- **Specifically Negotiated License Rights.** This right pertains whenever the standard license arrangements are modified to the mutual agreement of the contractor and the Government. In this case, the exact terms are spelled out in a specific license agreement unique to each application.

- **Small Business Innovative Research (SBIR) Data Rights.** All technical data or computer software generated under a SBIR contract. Government users cannot release or disclose outside the Government except to Government support contractors.

- **Commercial Technical Data License Rights.** Applies to technical data related to commercial items (developed at private expense). Managed in the same manner as Limited Rights.

- **Commercial Computer Software Licenses.** Applies to any commercial computer software or software documentation. Managed as specified in the commercial license offered to the public.

Only under very unique circumstances does the Government acquire title to or ownership of technical data or computer software developed under DoD contracts – even if the Government funded 100% of the development. Instead, the Government acquires a license to use, release, or disclose that technical data or computer software to persons who are not Government employees. Therefore, the DoD often negotiates over license rights and not ownership of technical data or computer software to be delivered under a contract. A Program Manager must ensure that all Technical Data and Computer Software and related license rights required for procurement and sustainment of a system are available throughout a system’s life cycle.

The DFARS, subpart 227.71 (rights in technical data) prescribes policies and procedures for the acquisition of technical data and the rights to use, modify, reproduce, release, perform, display, or disclose technical data. Statutory references Title 10 U.S.C. § 2320 and Title 10, U.S. Code, § 2321 also provide additional information. Other resources for learning about data rights include:

- DAU continuous learning module CLE 068 “Intellectual Property and Data Rights”
- 2013 Better Buying Power Trifold – “Understanding and Leveraging Data Rights in DoD Acquisitions”
- Army Data and Data Rights Guide (D&DR Guide), 2015
CH 6–3.7 Common IT Standards

The DoDI 8301.01, "Information Technology Standards in the DoD" is the overarching policy for IT standards in order to promote interoperability, information sharing, reuse, portability, and cybersecurity within the DoD. It is policy that DoD-approved and adopted standards are listed in the DoD IT Standards Registry (DISR), which enables centralization and transparency of available and applicable standards across the Department. To request an account, please fill out the form located here.

CH 6–3.7.1 Enterprise Architecture

All DoD architectures, including warfighter, intelligence, business, and component enterprise architectures, are part of the DoD Enterprise Architecture (EA). The DoD EA is defined as a federation of descriptions that provide context and rules for accomplishing the mission of the Department. These descriptions are developed and maintained at the Department, Capability Area, and Component levels and collectively define the people, processes, and technology required in the "current" and "target" environments, and the roadmap for transition to the target environment. As the Secretary of Defense's principal staff assistant for IT and information resources management, the DoD Chief Information Officer (DoD CIO) develops, maintains, and facilitates the use of the DoD EA to guide and oversee the evolution of the Department's IT-related investments to meet operational needs.

To comply with the enterprise architecture:

- Follow the DoD Architecture Framework (DoDAF) guidance in creating architectural views. This guidance is met by creating an architecture that captures the specific data needed to support decision making. The specific data is predicated by explicitly identifying the intended use and scope of the architecture in question. DoDAF guidance can be accessed through the Office of the Deputy Chief Management Officer's DoDAF webpage.
- Meet the DODAF Meta-model (DM2) Physical Exchange Specification (PES) requirements for sharing/reusing architecture data. DODAF Meta-model (DM2) guidance can be accessed from the DCMO's DODAF Meta-model webpage.
- When building systems, requests for proposals (RFPs) and contract statements of work (SOWs) should be reviewed as part of approved acquisition processes to ensure IT standards established in ICDs, CDDs, CPDs or Problem Statements are translated into clear contractual requirements.

CH 6–3.7.1.1 Open Systems Architecture

PMs are responsible for applying open systems approaches in product designs where feasible and cost-effective. Open systems and modular architectures provide valuable mechanisms for continuing competition and incremental upgrades, and to facilitate reuse across the joint force. PMs should use open systems architecture design principles to support an open business model (see paragraph 6a(4) in Enclosure 2 of the DoDI 5000.02).

CH 6–3.7.1.2 Business Enterprise Architecture (BEA)

The Business Enterprise Architecture (BEA) is the enterprise architecture for the DoD Business Mission Area and reflects DoD business transformation priorities; the business capabilities required to support those priorities; and the combinations of enterprise systems and initiatives that enable those capabilities. It also supports use of this information within an End-to-End (E2E) framework.

The purpose of the BEA is to provide a blueprint for DoD business transformation that helps ensure the right capabilities, resources and materiel are rapidly delivered to our warfighters – what they need, when they need it, where they need it, anywhere in the world. The BEA guides and constrains implementation of interoperable defense business system solutions as required by Title 10 U.S.C. section 2222. It also
guides information technology investment management to align with strategic business capabilities as required by the Clinger-Cohen Act, and supports Office of Management and Budget (OMB) and Government Accountability Office (GAO) policies.

The Strategic Management Plan (SMP), Functional Strategies as developed by the appropriate DoD Principal Staff Assistants and the Organizational Execution Plans (OEP) as developed by DoD Components are the drivers of BEA release content.

**CH 6-3.7.2 Audit Readiness and Audit Standards**

DOD's financial management has been on GAO's High Risk List since 1995 because of pervasive deficiencies in financial and related business management systems, processes, and controls. Congress has mandated a full audit of DOD’s FY2018 financial statements, the results of which must be submitted to Congress by March 31, 2019. A critical piece in aiding the Department to achieve financial auditability is the Comptroller's Financial Improvement and Audit Readiness (FIAR) Plan and the accompanying FIAR Guidance. The FIAR Guidance serves as a standard reference guide for existing and new users involved in all audit readiness initiatives across the Department. The DoD Comptroller’s FIAR Directorate has also published an extensive and helpful resource of tools, templates and work products.

The FIAR Guidance contains discussion of common critical standards in order to aid the Department in achieving auditability, which ultimately impacts the requirements and configurations of IT systems as they are developed, deployed and managed:

- **Federal Managers' Financial Integrity Act of 1982 (FMFIA)**, which established overall requirements for management’s responsibilities with respect to internal controls.
- **The Chief Financial Officers (CFO) Act of 1990 (Public Law 101-576)**, the purpose of which is to drive improvement of government financial management and creates standards of performance and disclosure.
- **The Federal Financial Management Improvement Act of 1996 (FFMIA)**, which requires agencies to incorporate applicable federal accounting standards into their financial management systems, maintain A-123 compliant systems, and regularly and report on those systems.
- **The Federal Information Security Modernization Act of 2014 (FISMA 2014)** requires the head of each agency to implement policies and procedures to cost-effectively reduce information technology security risks to an acceptable level, and emphasize cybersecurity.
- **The GAO’s “Green Book”** or Standards for Internal Control in the Federal Government sets the standards for an effective internal control system for federal agencies. An entity uses the Green Book to help achieve its objectives related to operations, reporting, and compliance.
- **Federal Information System Controls Audit Manual (FISCAM)** provides a methodology for performing IT / IS control audits of federal and other governmental entities in accordance with professional standards. The FISCAM is the basis on which DoD IT / IS are assessed in accordance with the FIAR Guidance.
- **Defense Finance and Accounting Service – Financial Management Systems Requirements Manual General and Administrative Information (FFMIA) 7900.4-M “Blue Book” enables compliance with the FFMIA.**

**CH 6-3.7.3 Standard Financial Information Structure (SFIS)**

The Standard Financial Information Structure (SFIS) is a comprehensive data structure that supports requirements for budgeting, financial accounting, cost/ performance, and external reporting needs across the DoD enterprise. SFIS standardizes financial reporting across DoD and allows revenues and expenses to be reported by programs that align with major goals, rather than basing reporting primarily on appropriation categories. It also enables decision-makers to efficiently compare programs and their associated activities and costs across the department and provides a basis for common valuation of DoD programs, assets, and liabilities.

**CH 6-3.7.4 Item Unique Identification**

Item Unique Identification (IUID) is an international standards-based approach adopted by the DoD and its implementation is driven by and required by DoD 8520.03, "Unique Identification (UID) Standards for
Supporting DoD Net-Centric Operations. IUID makes the acquisition, repair, and deployment of items faster and more efficient through achievement of information sharing, visibility, assurance, and interoperability. IUID is required for all new DoD acquisitions; items the government already owns (i.e., legacy items); and government furnished property meeting any one of the following criteria:

- the item has a line item acquisition cost in its contract of $5,000 or more
- the item is or will be serially managed by the DoD
- the item is or will be controlled or mission essential
- permanent identification is or will be wanted for any other reason

IUID may apply differently for embedded systems. Items requiring IUID must be assigned a globally unique, permanent unique item identifier, or UII, and the UII registered, along with other item identifying information, in the DoD IUID Registry. Tools and guidance for implementing IUID are available in the IUID Toolbox.

CH 6–3.8 Interoperability

Interoperability, guided by the DoDI 8330.01, "Interoperability of Information Technology (IT), Including National Security Systems (NSS)", is the ability of systems, units, or forces to provide data, information, materiel, and services to, and accept the same from, other systems, units, or forces and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together. Information Technology (IT) and NSS interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchange of information as required for mission accomplishment. Interoperability is more than just information exchange. It includes systems, processes, procedures, organizations and missions over the life cycle, and it should be balanced with IA.

Supportability for IT systems and NSS is the ability of systems and infrastructure components, external to a specific IT or NSS, to aid, protect, complement, or sustain the design, development, testing, training, or operations of the IT or NSS to achieve its required operational and functional capabilities.

IT and NSS interoperability and supportability needs, for a given capability, be identified through:

- The Defense Acquisition System (as defined in the DoD 5000 series issuances)
- The Joint Capabilities Integration and Development System process
- The DBS Problem Statement Process
- The Doctrine, Organization, Training, Materiel, Leadership and Education Personnel and Facilities (DOTMLPF) change recommendation process

CH 6–3.8.1 Interoperability Requirements and Verification

For all information technology, measurable interoperability requirements must be identified, formally validated through NR KPP certification, and then formally tested through an interoperability certification process. The Joint Interoperability Test Command (JITC) produces an Interoperability Process Guide which outlines the procedures and documentation required for Joint Interoperability Test and Certification, waiver processing, and associated processes and procedures. It also addresses interoperability test and certification based on the Net-Ready Key Performance Parameter (NR KPP). More on the role of JITC can be found in CH 8 Section 2.3.4.1.

Interoperability requirements must be documented in a succinct, measurable, and testable manner as an NR KPP. The NR KPP must address information requirements, information timeliness, and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange.

The ISP is a key document in achieving interoperability certification. The ISP describes IT and information needs, dependencies, and interfaces for programs. It focuses on the efficient and effective exchange of information that, if not properly managed, could limit or restrict the operation of the program in accordance with its defined capability. Interoperability testing is further described in CH 8 Section 3.7.6.
CH 6–3.8.1.1 Net-Ready KPP

Net-ready attributes determine specific criteria for interoperability, and operationally effective end-to-end information exchanges which are traceable to their associated operational context, and are measurable, testable, and support efficient and effective T&E.

- The NR KPP identifies operational, net-centric requirements in terms of threshold and objective values for MOEs and MOPs. The NR KPP covers all communication, computing, and EM spectrum requirements involving information elements among producer, sender, receiver, and consumer. Information elements include the information, product, and service JCIDS Manual 12 February 2015 D-E-3 Appendix E Enclosure D exchanges. These exchanges enable successful completion of the warfighter mission or joint business processes.
- The NR KPP includes three attributes derived through a three step process of mission analysis, information analysis, and systems engineering. These attributes are then documented in solution architectures developed according to the current DODAF standard.
  - Attribute 1: Supports military operations
  - Attribute 2: Is entered and managed on the network
  - Attribute 3: Effectively exchanges information

The most recent JCIDS Manual dated 12 February 2015 added a Certification Guide for the Net-Ready KPP (NR KPP) and expanded the Content Guide for the NR KPP with the majority of the content from CJCSI 6212.01F. Remaining content from CJCSI 6212.01F related to roles and responsibilities is consolidated into CJCSI 5123.01G.

CH 6–3.8.2 Interface Design and Management

One of the most challenging aspect of IT system development in DoD deals with system interfaces. In a net-centric environment, the shift is to a "many-to-many" exchange of data, enabling many users and applications to leverage the same data extending beyond the previous focus on standardized, predefined, point-to-point interfaces. Hence, the objectives are to ensure that all data are visible, available, and usable when needed and where needed to accelerate decision cycles. Many-to-many exchanges of data occur between systems, through interfaces that are sometimes predefined or sometimes unanticipated. Metadata is available to allow mediation or translation of data between interfaces, as needed.

PMs should have written agreements with any interface partners (i.e., such as between DFAS-DLA, or between the Air Force and DFAS) which indicate the agreement made and requirements documented for the subject program and those programs necessary for information support.

Typically, these interface dependencies will be documented in Information Support Plans (ISPs) for both System A (the information recipient) and System B (the information provider) though could be documented differently depending on the program’s document tailoring strategy. More information on the interface management process is located in CH 4.3 Section 4.1.8.

CH 6–3.8.3 Modeling & Simulation

DoD Directive 8000.01, “Management of the Department of Defense Information Enterprise (DoD IE)”, encourages pilots, modeling and simulation (M&S), experimentation, and prototype projects, appropriately sized to achieve desired objectives, and not be used in lieu of testing or acquisition processes to implement the production version of the information solution. This concept equally applies to IT systems, which may pilot and prototype differently than weapons systems but may find it just as beneficial.

M&S tools can be used by multiple functional area disciplines during all life-cycle phases. Modeling is essential to aid in understanding complex systems and system interdependencies, and to communicate among team members and stakeholders. Simulation provides a means to explore concepts, system characteristics, and alternatives; open up the trade space; facilitate informed decisions and assess overall system performance.

The Director, Systems Analysis within the Office of the Deputy Assistant Secretary of Defense for Systems Engineering guides the M&S community. More detailed M&S procedures are described in detail
in CH 3 Section 2.4.2. Another resource is the DoD Modeling and Simulation Coordination Office, or M&SCO. M&S specific to test and evaluation is located in CH 8 Section 3.7.7.

CH 6–3.9 Enterprise Services
The Department of Defense is rapidly moving to a multi-provider Enterprise Cloud Environment to deliver the most innovative, efficient, and secure information and IT services in support of the Department's mission, anywhere, anytime, on any authorized device. The DoD CIO is accelerating and synchronizing efforts that create enterprise-wide capabilities and Enterprise Services while eliminating the unnecessary duplication of capabilities.

CH 6–3.9.1 Joint Information Environment
DoD, through the CIO's Strategy for Implementing the Joint Information Environment (JIE) is transitioning to a single, joint, secure, reliable and agile command, control, communications and computing (C4) enterprise information environment.

The JIE is a construct that facilitates the convergence of the DoD's multiple networks into one common and shared global network. The intent is to provide enterprise services such as email, Internet/Web access, common software applications, and cloud computing. Primary objectives behind this transition are increased operational efficiency, enhanced network security and cost savings through reduced infrastructure and manpower.

The JIE is a fundamental shift in the way the DoD will consolidate and manage IT infrastructure, services, and assets in order to realign, restructure, and modernize how the Department's IT networks and systems are constructed, operated, and defended. JIE will consolidate and standardize the design and architecture of the Department's networks. The JIE represents the DoD migration from military service-centric IT infrastructures and capabilities, with their mixture of disparate networks and applications, to enterprise capabilities based on common infrastructure and shared services to support Joint needs. These needs include networks, security services, cyber defenses, data centers, and operation management centers. Consolidation and standardization will result in a single, reliable, resilient, and agile information enterprise for use by the joint forces and mission partners. The key attributes of the JIE include:

- Shared JIE technology infrastructure: a network that is defendable and virtually accessible from any location globally, strategic to tactical locations; DoD level consolidation of data centers and network operations centers; a single security architecture; and the use of enterprise services.
- The JIE infrastructure will look, feel and operate by common standards regardless of service provider and/or use (i.e., mission specific utilization) and will apply common tactics, techniques and procedures developed at the enterprise level.
- Capabilities required across DoD to enable information sharing, collaboration and interoperability will be provisioned as enterprise services. Email, Web access, mass data storage and data analytics for decision support will be provided to any access point.
- The JIE effort does not preclude the Navy, for example, or any other Service from becoming a service provider for one or more designated enterprise services or infrastructure capabilities. As such, the Navy could be called upon to support the provisioning of enterprise service(s) for the entire DoD.
- Services and Agencies are beginning to adopt JIE standards for existing programs of record and adapt to JIE standards and requirements in future IT modernization.
- Services and Components that operate and maintain portions of the shared IT infrastructure (i.e., switches, servers, routers, etc.) will do so in accordance with the appropriate IT Technical Authority through the Joint Information Environment Technical Synchronization Office (led by the Defense Information Systems Agency), and with operational direction provided by U.S. Cyber Command.

CH 6–3.9.1.1 Joint Regional Security Stacks (JRSS)
DISA's joint regional security stacks (JRSS) represents a single security architecture; it constitutes a suite of equipment that performs firewall functions, intrusion detection and prevention, enterprise management,
virtual routing and forwarding (VRF), and provides a host of network security capabilities. JRSS is a cornerstone of JIE implementation and part of a larger modernization effort to upgrade the bandwidth capacity of the Defense Information Systems Network (DISN). Installation is in progress at ten of the eleven JRSS sites planned in the continental United States (CONUS) and five sites planned outside CONUS (OCONUS). JRSS familiarization training is available through DISA. The benefits for PMs and other implementers of IT are as follows:

- JRSS offers increased visualization into the network. Deploying JRSS enables the department to inspect data, retrieve threat and malware data on the network and troubleshoot, and then patch, protect, and defend the network.
- JRSS will improve the effectiveness and efficiency of the network by ensuring that there is sufficient capacity to support the transition of services and capabilities from being hosted locally by the military departments.
- JRSS will support the concepts of the JIE and specifically will reduce duplication of security standards.

**CH 6–3.9.2 Cloud Computing**

In its simplest sense, cloud computing is the delivery of IT as a service. Instead of purchasing an IT system and all its necessary peripherals that is maintained on premise, by utilizing cloud computing, an organization can acquire an IT capability or set of capabilities (aka Cloud Service Offerings (CSOs)) that are accessed from a network. The IT needed to create, store, and deliver the capability is maintained off-site by Cloud Service Providers (CSPs). Cloud computing services can deliver more efficient IT than traditional acquisition approaches. Organizations pay for the IT capability or service based on the amount of usage. A formal definition is provided in the National Institute of Standards and Technology (NIST) Definition of Cloud Computing Special Publication 800-145:

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

As applications and capabilities are moved to the Cloud, DoD PMs will select CSOs that are offered in one of three Service Models and four Deployment Models:

**Service Models:**

- **Infrastructure as a Service (IaaS):** Processing, storage, networks, and other fundamental computing resources. Purchaser generally still has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).
- **Platform as a Service (PaaS):** Applications created using programming languages, libraries, services, and tools supported by the CSP. (This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources.) The purchaser does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
- **Software as a Service (SaaS):** Applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The purchaser does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

**Deployment Models:**

- **Public cloud infrastructures operate in a multi-tenant environment whose resources are allocated for the general public. Public clouds tend to be large and provide economies of**
scale for their customers. However, security and privacy concerns are heightened because any individual or organization can potentially access the same cloud infrastructure.

- Private cloud infrastructures are operated only for an individual organization. The organization can leverage the scalability and performance aspects of cloud computing, but the infrastructure is isolated from that of other organizations, improving security and privacy. Because of their specialized nature, private clouds can be just as costly as dedicated data centers.
- Community cloud infrastructures are private clouds provisioned for a specific community of interest with shared concerns, such as a government-only cloud.
- Hybrid cloud infrastructures are combinations of any two or more of the other cloud infrastructures.

Figure 6 compares these three models to the traditional (on premise) data center model, where DoD provides all of the infrastructure components.

**Figure 6: Cloud Computing Services Models Overview and Responsibilities**

![Cloud Computing Services Models Overview and Responsibilities](image)

### CH 6–3.9.2.1 Interpreting Cloud Policy and Guidance

The DoD CIO, through a December 15, 2014 memorandum, enumerates DoD Component responsibilities when acquiring commercial cloud services to include the following:

- Provide an analysis of the cloud services requested using the DoD CIO-Enterprise IT Business Case Analysis (BCA) template as a guide;
- Consider DISA provided cloud services as an alternative in the BCA; and
- Have the approval of the Component CIO; provide a copy of the BCA to the DoD CIO.

DoD PMs should make and document a "cloud-or-not-cloud" determination as part of the IT BCA process using the following information as a guide:
On Demand Self-service: The CSP may provision the CSO without human interaction;

Broad Network Access: The CSO is available to a variety of devices over a wide range of networks using standard protocols;

Resource Pooling: The CSP’s computing infrastructure may be provisioned and shared among multiple tenants without their knowledge;

Rapid Elasticity: The CSO has the ability to expand and contract to meet the demands of the customer’s application.

Measured Service: The CSP has the ability to meter the resource usage with enough detail to support customer requirements.

Additional cloud policy and guidance that you must follow when acquiring and implementing cloud services include:

**DoD Cloud Computing Security Requirements Guide (CC SRG):** was built upon the DoD Instruction 8510.01, Risk Management Framework (RMF) for DoD Information Technology to integrate with the DoD RMF Authorization Process and Office of Management and Budget (OMB) policy regarding federal government use of cloud computing.

The CC SRG is an essential guide to identify the cybersecurity controls and information impact levels (IILs) for hosting DoD missions in CSOs up to and including SECRET, based on the type of data to be hosted in the CSO. The CC SRG establishes the baseline security requirements for DoD PMs and their Authorizing Officials (AOs) and must be followed when contracting for and implementing systems and applications using DoD and non-DoD CSOs regardless of service or deployment models. The CC SRG also identifies the roles and responsibilities that DoD Mission Owners, PMs, CSPs, and the DoD PM’s Cybersecurity Service Provider (CSSP) play in operating and securing cloud hosted systems. DoD PMs that offer DoD owned and operated cloud services are subject to the same regulations as all DoD information systems, and must comply with the DoD CC SRG.

Defense Information Systems Agency (DISA) as the Department’s Risk Management Executive, uses the CC SRG to oversee the required DoD cybersecurity assessment of a CSP’s CSO that results in the issuance of a DoD Provisional Authorization (DoD PA). The DoD PA is an assessment indicating that the CSO is potentially suitable for use up to an indicated impact level as defined within the CC SRG. The latest version of the CC SRG can always be found [here](#).

**DFARS Subpart 239.7 – Cloud Computing** implements policy developed within the DoD CIO and the CC SRG for the acquisition of cloud computing services. The provision, 252.239-7009, "Representation of Use of Cloud Computing," must be used in solicitations for information technology services. This allows the offeror to represent their intention to utilize cloud computing services in performance of the contract or not. The clause 252.239-7010, "Cloud Computing Services," must be used in solicitations and contracts for information technology services. This provides standard contract language for the acquisition of cloud computing services, including access, security, and reporting requirements.

The DFARS states, that the contracting officer should only award a contract to acquire cloud computing services from any CSP (e.g., contractor or subcontractor, regardless of tier) that has been granted a DoD PA with two exceptions: (a) DoD CIO waiver the requirement or (b) CSO is hosted in a DoD facility and has DoD PA prior to operational use.

DoD PMs must provide the Contracting Officer all detailed requirements associated with this clause and others that need to be included in the purchase request when contracting for CSOs.

**CH 6–3.9.2.2 Cloud Service Acquisition Process Steps**

There are four major inter-related steps to follow when acquiring cloud services for the DoD.

**Step 1: Determine Appropriate Information Impact Levels and Categorize Mission and Data Risk.**

When acquiring cloud services, DoD PMs need to consider both the impact of data loss/compromise (security) and the priority of the service relative to the primary mission of the DoD (Mission Impact). The
focus is on the CSO not the provider of the service who may offer services that are eligible at different information impact levels. The following provides a summary of the four information impact levels defined in the CC Security Requirements Guide (SRG) coupled with some of the distinguishing requirements and characteristics:

- **Level 2.** The system processes DoD information that has been cleared for public release; information that has been released through the Freedom of Information Act (FOIA); and information available to the public even if it requires a login. Level 2 applies to non-NSS only.

- **Level 4.** The system processes DoD Controlled Unclassified Information (CUI) (i.e., For Official Use Only (FOUO), Moderate and Sensitive Personally Identifiable Information (PII) (i.e., social security numbers, alien ID and other immigration documents, passport numbers, driver’s license numbers, vehicle identification numbers, and license plates), Non-Appropriated Fund (NAF) data, and other non-CUI mission critical systems that are not NSS systems.

- **Level 5.** The system processes CUI requiring higher protection, mission essential, critical infrastructure (military or civilian), deployment and troop movement, International Traffic in Arms Regulation (ITAR) data, or unclassified nuclear data. It also includes highly sensitive PII which could include Protected Health Information (PHI), law enforcement, and other data that contains sexual assault information.

- **Level 6.** Level 6 accommodates information that has been determined: (i) pursuant to Executive Order 12958 as amended by Executive Order 13292, or any predecessor Order, to be classified national security information; or (ii) pursuant to the Atomic Energy Act of 1954, as amended, to be Restricted Data (RD). Only information classified as SECRET, in accordance with the applicable executive orders, is applicable to this level.

**Step 2: Identify Approved CSOs and Roles and Responsibilities.**

Once the DoD PM and their AO determines what types of cloud services are to be acquired (IaaS, PaaS, or SaaS) and the Information Impact Level the CSP needs to support, the appropriate cloud service alternatives can be evaluated and the required IT BCA can be performed. DoD PMs then select CSOs based on their security posture and the risk tolerance of the PM and their AO. The PM should identify existing approved CSOs that have a current PA from DISA by referring to the DoD Cloud Catalog (CAC required to access) maintained by DISA.

Moving to the cloud underscores the need for PMs to understand the distinction between what is and is not provided and addressed by the CSP. DoD PMs need to clearly identify roles and responsibilities as they will vary depending on the service model as illustrated in Figure 6 above. Therefore, a fundamental consideration for DoD PMs should be determining the appropriate contractual relationships between all parties to ensure that mission capabilities can be met from a holistic systems view.

**Step 3: Ensure Cyber Defense.**

DoD PMs that acquire or use cloud services remain responsible for ensuring end-to-end security and protection of their system/application IAW the CC SRG. As the DoD strives to maximize the use of commercial cloud computing, the DoD Information Network (DODIN) perimeter must continue to be protected against cyber threats from external connections.

CSOs hosting IIL 4/5 must be connected to the DODIN through a CAP or other boundary defense mechanism that has been approved by DoD CIO. CSOs hosting IIL 2 will connect through the Internet. DoD PMs and their AOs must ensure that prior to transitioning to a CSO, a supporting Cyber Defense Service Provider (CSSP) has been identified and confirmed; and the required monitoring capabilities must be functional prior to operational use.

**Step 4: Cloud Service Registration and Reporting**

DoD PMs must report their cloud computing activities as follows:

- **Registration in DISA System Network Approval Process (SNAP):** DoD PMs must register all CSOs that they plan on acquiring or are using, regardless of IIL or the network connection or CAP.
requirement, in the DISA's SNAP system in the Mission Owner (Cloud IT Project) Module. (NOTE: registration is required, see instructions on the SNAP website for details).

- **Registration in DITPR:** DoD PMs must register use of the CSP's CSO in the DoD Information Portfolio Registry (DITPR).
- **Investment Reporting via SNaP-IT:** Program Managers must analyze cloud computing options and report cloud service funding investments during the course of DoD budget and acquisition processes for each CSO as follows:
  - Ensure that an investment line item has been created in Select and Native Programming Data Input System – Information Technology (SNaP-IT) for each investment in a CSO;
  - Report all funding related to cloud computing by Deployment Model and Service Model for the Prior Year, Current Year and Budget Year.

### CH 6–3.9.2.3 Contracting for Cloud Services

Contracting for commercial CSOs brings additional risks and concerns that could adversely affect the mission but may not be apparent and are not typically addressed in traditional contracting best practices. For example, typical vendor contract terms and conditions may not be detailed enough concerning items that are expected to be encountered once operations and services begin, i.e., operations, maintenance, and the cybersecurity of the DoD system residing in the CSO. Other concerns include ensuring that the Inspector General and Law Enforcement are able to perform their responsibilities. Each DoD PM should coordinate with their legal counsel, privacy, and procurement offices when they move IT services to the commercial cloud, and ensure compliance with Federal Records Management, and other OMB and DoD requirements.

Identifying and determining risk is an integral factor in cloud contracting decisions. Cybersecurity (relative to cloud) is concerned with risks to the DODIN (CSO/DODIN risks) and risks specific to a mission and its data (CSO/mission risk). The CC SRG is the primary source governing the selection, accreditation, and ongoing accreditation and use of cloud services within the DoD. Although the CC SRG is quite comprehensive, the DoD PM must take the time to comprehend it in order to determine if additional requirements need to be reflected in the SLA or contract.

Initial decisions regarding CSO/DODIN risk are normally made through the DoD PA assessment and authorization process. Ongoing adherence to the CC SRG is periodically reviewed and the CSO's network behavior is being continuously monitored in order to identify if there is an increase in CSO/DODIN risk; the DoD PA and/or access to the CSO may be terminated depending on the severity of risk.

Initial decisions regarding CSO/mission risk are made through the mission owner’s agency ATO process. Remember, a CSO with a DoD PA does not eliminate the requirement for a given application using the CSO to have an ATO (or IATT) prior to commencing operations. For example, prior to contract award the AO should review DoD PA artifacts to understand the risks that the mission may inherit and request that compensating controls be implemented by the CSP prior to obtaining an ATO. The compensating controls must be reflected in the SLA/contract as well as processes to assure they remain valid.

Therefore, it is essential that DoD PMs determine exactly what they are responsible for as well as the roles and responsibilities of all other stakeholders that may include the CSP, the Contractor if not the CSP, Sub-contractor, an outsourced 3rd party integrator or CSP, cybersecurity personnel, or other entities. DoD PMs must fully understand, describe and negotiate their key expectations and ensure that they are specifically addressed in the contract/Task Order (TO), Acquisition Plan, Contract Performance Work Statement (PWS) or SLA for cloud computing contracts.

PMs and appropriate staff should become familiar with the DFARS Subpart 239.76 (Cloud Computing), and the associated DFARS 252.239-7009 Provision and DFARS 252.239-7010 Clause, the supporting Procedures, Guidance and Instructions (PGI) 239.76 – Cloud Computing and the CC SRG.

Table 5, “Information and/or actions required for DoD PMs” should be read in conjunction with the DFARS subpart, provision and clause, PGIs and the CC SRG. It identifies the specific information and/or requirements the PM needs to provide the Contracting Officer (CO) to enable the CO to execute a
contract that protects DoD equities and minimizes risk. In addition, activities that require PM coordination and risk assessment decisions with the PM’s AO or other DoD entities are identified.

Table 5: Information and/or actions required for DoD PMs

<table>
<thead>
<tr>
<th>Description</th>
<th>Information and/or actions required for DoD PMs</th>
</tr>
</thead>
</table>
| **General Procedures for Cloud Services** | • Determine Information Impact Level (IIL) as detailed in the CC SRG.  
• Provide written justification as needed by CO. |
| **Government Data & Government-Related Data** | • Identify, document, and provide CO with unambiguous descriptions and formats of Government data and Government-related data need to enforce all terms in clause where, “Government data and Government-related data” are referenced in DFARS 252.239-7010.  
• These descriptions and formats of Government data and Government-related will be required by CO. |
| **Security Requirements – Change in Representation (DFARS 252.239-7010 (b) (1))** | • Post contract award; if the contractor notifies the CO of a change in DFARS Provision 252.239-7009 then, it is likely that the entire approach will require reevaluation.  
• In collaboration with AO, reevaluate the proposed approach and determine if the change is acceptable.  
• Provide written notice and/or justification to support approval or disapproval decision to CO. |
| **Security Requirements – Waiver (DFARS 252.239-7010 (b) (2))** | • Collaborate with AO and DoD CIO to determine what specific requirements of the CC SRG may/have been waived.  
• Provide CO with necessary documentation needed to specify extent and conditions of the DoD CIO waiver. |
| **Location of Data – (DFARS 252.239-7010 (b) (3))** | • Collaborate with AO to determine (only for Level 2 or Level 4 data) if it is permitted to maintain Government data at a location outside the 50 States, the District of Columbia, and outlying areas of the United States.  
• Provide written justification as needed by CO. |
| **Limitations on Access, Use and Disclosure (DFARS 252.239-7010 (c) (1))** | • Collaborate with AO to review and determine and unambiguously document if any access to or use of Government Data or Government-related Data requested or specified by contractor is permissible and if so under what limitations and/or conditions.  
• Provide CO with documentation authorizing access. |
| **Cyber Incident Reporting (DFARS 252.239-7010 (d))** | • Identify a Government point of contract (POC) for CO to contact if a cyber-incident occurs in connection with the cloud computing services being provided.  
**If a cyber-incident occurs:**  
• Procedures should be developed (to include, Mission Owner, Cybersecurity Service Provider (CSSP), and Contractor) to collect, preserve and protect Incident Information; these processes will vary depending on service model (IaaS, PaaS and SaaS).  
• With the AO, CSSP, and the Contractor, assess and determine the potential impact of the cyber incident and response. |
<table>
<thead>
<tr>
<th>Description</th>
<th>Information and/or actions required for DoD PMs</th>
</tr>
</thead>
</table>
| Malicious Software DFARS 252.239-7010 (e) | • Collaborate with AO and other DoD entities to produce detailed instructions on submitting malicious software that was/may-have-been discovered in connection with a reportable cyber incident.  
• Provide the CO with the specific instructions produced. |
| Cyber Incident – Requesting Media and Data DFARS 252.239-7010 (f) | • Collaborate with AO and other DoD entities to determine if the media that was preserved and/or the data that was collected (when a cyber-incident was discovered) are required by the DoD.  
• If required, instruct CO to request media and data from the contractor. |
| Cyber Incident – Access to Information or Equipment DFARS 252.239-7010 (g) | • Collaborate with AO and other DoD entities to determine if access to additional information or equipment is needed to conduct forensic analysis.  
• If needed, instruct CO to request access to additional information and/or equipment. |
| Cyber Incident – Damage Assessment DFARS 252.239-7010 (h) | • Collaborate with AO and other DoD entities to determine if damage assessment is required.  
• If damage assessment is required, inform CO to request damage assessment information from contractor.  
• Upon completion of damage assessment activities, provide the CO with a report documenting all findings that will be included in the contract files. |
| Records Management and Facility Access DFARS 252.239-7010 (i) | • When acquiring SaaS, provide a records retention schedule to the CO to be incorporated in the contract that includes, but is not limited to, secure storage, ability to retrieve, and proper disposition of all federal records.  
• When acquiring IaaS/PaaS, maintain a copy of the Contractor’s and/or CSP’s records retention policies for Government related data. |
| Records Management – Format of Data DFARS 252.239-7010 (i) (1) | • Collaborate with AO and all other related DoD stakeholders to provide the CO with unambiguous description of formats of Government data and Government-related data needed to enforce the terms in clause. |
| Records Management – Contract Closeout DFARS 252.239-7010 (i) (2) | • Collaborate with AO and, if necessary, the Component Records Management Officer (CMRO), to determine how Government Data and Government-related data is to be handled during contract closeout.  
• Provide CO with unambiguous description of how contractor is to transfer, retain, or dispose and confirm disposal of Government Data and Government-related data as part of contract closeout needed to enforce the terms in clause. |
| Records Management – Required Accesses to … DFARS 252.239-7010 (i) (3) | • Collaborate with AO and all other stakeholder DoD entities to identify and ensure that all Government or its authorized representatives have determined and documented what physical, system, and/or system-wide accesses and response timeframes the contractor will need to provide in order to support their lawful activities.  
• Provide CO with unambiguous description of all accesses and timeframes required in the contract/SLA. |
<table>
<thead>
<tr>
<th>Description</th>
<th>Information and/or actions required for DoD PMs</th>
</tr>
</thead>
</table>
| **Notification Of Third Party Access Requests**<br>DFARS 252.239-7010 (j) | - Identify the government point of contact (POC) responsible for coordinating the response to any subpoena or other third party access received by the contractor providing the cloud service.  
- Provide CO with the government POC.  
**If third party access request is received:**  
- Coordinate the response with the DoD mission or data owner. |
| **Spillage**<br>DFARS 252.239-7010 (k) | - Identify the contractor POC and government POC to contact if any spillage occurs regarding the cloud service being provided.  
- Provide CO with the POCs and procedures needed to enforce the terms in clause.  
- Ensure that agency procedures for addressing a spillage are documented.  
**If spillage occurs:**  
- Follow agency procedures. |
| **Subcontracts**<br>DFARS 252.239-7010 (l) | - Provide CO with requirements related to flow down when contracting for PaaS or SaaS which leverages an IaaS or PaaS from a third party CSP. |
| **Contractor Terms And Conditions - Terms Of Service (ToS)**<br>Subpart 239.7601-1 (a) | - Collaborate with AO to review contractor’s Terms of Service and produce document detailing where they may be found to impede or conflict with mission and cyber security requirements.  
- Provide CO with the document to ensure conflicts are resolved as part of the other processes the CO needs to perform in order to meet the intent of this Subpart. |
| **Inspection, Audit, Investigation Support**<br>Subpart 239.7601-1 (c) (3) | - Provide CO with requirements to support authorized activities regarding Government Data or Government-related Data, or CSO service model. |
| **Inspection, Audit, Investigation Search & Access**<br>Subpart 239.7601-1 (c) (4) | - Provide CO with requirements to support and cooperate with authorized activities’ system-wide search and access. |
| **Other Consideration – Cybersecurity Compliance CC – SRG** | - Collaborate with AO to ensure that cybersecurity requirements or processes not otherwise addressed in the CC SRG and DoD PA assessment are documented. DoD PMs must ensure that issues identified throughout the life of the contract that may adversely impact CSO/mission risk, and thereby jeopardize the validity of the ATO, are addressed in the contract/SLA. For example, if DISA discovers that the CSP is not meeting on-going security requirements they will notify affected Mission Owners/PMs and work with the CSP to develop a corrective Plan of Actions and Milestones (POA&M).  
- Review DISA’s assessment of the Contractor’s corrective POA&M.  
- Collaborate with AO to make a risk determination with regard to their specific usage of the CSO and ATO.  
- Collaborate with AO and CO to determine if contracting action to incorporate the CSP’s POA&M is needed; annotate contract files as needed. |
In addition to the specific information and/or activities previously identified that DoD PMs need to provide, there are other considerations that could adversely affect the mission. Table 6, “Contracting Considerations for DoD PMs” details areas that should be included in any risk calculus, as well as the cost/benefit tradeoffs and risk analysis that have been identified by developing the business case analysis.

<table>
<thead>
<tr>
<th>Description</th>
<th>Information and/or actions required for DoD PMs</th>
</tr>
</thead>
</table>
| **Change In CSP Ownership CC – SRG** | - Collaborate with AO to determine how to address the impact of a change of ownership of the CSP. If such change necessitates off-boarding and retrieval of information/data, produce document that describes how the Contractor is to transfer, retain, or dispose and confirm disposal of Government Data and Government-related data.  
  - Provide CO with the document so that off-boarding processes can be reflected in the contract/SLA. |
| **Disaster recovery (DR) and Continuity of Operations (COOP)** | - As a best business practice, require that the Contractor (CSP or third party) plans for Disaster Recovery (DR) and Continuity of Operations (COOP) and implement their infrastructures to support it |
| **Exit Process** | - Provide CO with unambiguous document describing how contractor is to transfer, retain, or dispose and confirm disposal of Government Data and Government-related data and/or migrate applications upon completion or termination of the contract.  
  - Provide CO with the document so that close-out processes can be reflected in the contract/SLA. |

Table 6: Contracting Considerations for DoD PMs

<table>
<thead>
<tr>
<th>Description</th>
<th>Contracting Considerations for DoD PMs</th>
</tr>
</thead>
</table>
| **Banner** | - Banner language provides consent for the Department to view any content on the system without a warrant  
  - When acquiring software as a service, consider requiring the CSP to display DoD’s approved banner language prior to allowing a user access to the system |
| **Direct Contractual Relationship** | - Contractual liability to the government only exists with the prime contractor. When the DoD PM acquires a commercial service through an intermediary (e.g., system integrator, value added reseller), only the intermediary is accountable to the government. This reduces the contractual liability to the CSP acting as the subcontractor, but increases the risks to the government. |
| **Exit Strategy and Plan** | - Consider developing an interoperable strategy to move systems/applications from one CSP to another |
| **Indemnification** | - Consider requiring the CSP to indemnify the government against lawsuits; this protects the government when third parties sue the government for a tort when the CSP, not the government, was liable. |
| **Insurance** | - Consider requiring a CSP to use insurance services to pay for any costs stemming from a breach of DoD data (e.g., PII or PHI) or to replace any damages to the DoD system, including credit monitoring |
### Contracting Considerations for DoD PMs

<table>
<thead>
<tr>
<th>Description</th>
<th>Contracting Considerations for DoD PMs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ownership Rights</td>
<td>• Consider if any third party will own any aspects of assets that are applied for service provisioning</td>
</tr>
<tr>
<td>Training</td>
<td>• Consider whether a training and change management program might be needed to optimize implementation of security and cyber defense changes</td>
</tr>
</tbody>
</table>

### SLAs

DoD PMs should negotiate required service levels and expected performance with a key objective to reduce areas of potential conflict. Responsibilities and the appropriate support levels to meet requirements related to operations and maintenance of the environment, system management and administration services, logistics, performance, reliability/back-ups and disaster recovery functions should be clearly defined. DoD PMs should identify appropriate specific service level requirements and performance expected from a provider, how that performance will be measured, and what enforcement mechanisms will be used to ensure the specified performance levels are achieved in a SLA.

Table 7, “Requirements to be incorporated into SLAs” identifies the key requirements to be incorporated in DoD Cloud Contract SLAs, to help ensure the Contractor (and the CSP) meet the DoD’s contract objectives and CSOs perform effectively, efficiently, and securely:

Table 7: Requirements to be incorporated in SLAs

<table>
<thead>
<tr>
<th>DESCRIPTION</th>
<th>Requirements to be incorporated in SLAs</th>
</tr>
</thead>
</table>
| Roles And Responsibilities         | Define roles and responsibilities for the DoD, CSP, Contractor, Sub-contractor, 3rd party integrator or others to include:  
  • PMs, PM’s System Administrators  
  • NetOPS/Tier 2 & 3 support  
  • PM’s Cybersecurity (CS) entities, Cybersecurity Service Providers (CSSPs - Mission & Boundary CS)  
  • CSP’s CS entities, Trusted Internet Connection (TIC) support  
  • CSP’s or Contractor Audit or Forensic support  
  • Contractor’s Operations and Maintenance support |
<p>| Definitions/Terms                  | Provide a glossary of the key terms to supplement DFARS and CC SRG definitions to include continuity, outage, emergency, planned outage, unplanned outage, high availability, recovery, breach of service agreement, and other terms related to service performance and service reliability |
| Dates                              | Identify the dates when the contract/SLA is active or when measurement of the SLA will begin          |
| Accessibility                      | Provide a list of the accessibility standards, policies and regulations that must be met by the service |
| Availability                       | Identify availability requirements, e.g. percentage of time that the system or data will be available and usable |
| Data Location                      | Data location – list the geographic locations that data may be processed and stored, and if the Government can specify location requests |</p>
<table>
<thead>
<tr>
<th>DESCRIPTION</th>
<th>Requirements to be incorporated in SLAs</th>
</tr>
</thead>
</table>
| **Data Examination** | If the Government data is co-located with non-Government data, identify:  
- how the Contractor, and the CSP if not the Prime Contractor, will isolate the Government data into an environment where it may be reviewed, scanned, or forensically evaluated in a secure space  
- How access will be limited to authorized Government personnel identified by the CO, and without the Contractor’s involvement |
| **Records Management** | Records management – How and when the Contractor will retain or dispose of DoD records in the format specified as directed by the Contracting Officer |
| **Protection Of Personally Identifiable Information (PII) And Personal Health Information (PHI)** | Protection of Personally Identifiable Information (PII) is covered in the CC SRG. However, the table, “Privacy Overlay C/CE Not Included in FedRAMP M or FedRAMP+” identifies PII/PHI requirements that are not covered in the current DoD PA assessment.  
- In collaboration with the AO, define and produce document with requirements for the identified PII/PHI controls associated with: Access Control, Audit and Accountability, Security Assessment and Authorization; System Interconnections – Enhancement, Configuration Management, Incident Response, Media Protection, Personnel Screening, Risk Evaluations, System and Communications Protection, etc.  
- Provide CO with the document so that additional requirements can be reflected in the SLAs or contracts. |
| **Information Security; Security Performance** | The DoD PA does not assess certain security controls/control enhancements (C/CEs) that are identified in the CC SRG (e.g. availability of information related to continuous monitoring, incident response, vulnerability management, etc.).  
- Define and produce document describing responsibilities associated with the identified C/CEs for Access Control, Audit and Accountability, Device Identification and Authentication Enhancement and System and Communications Protection.  
- Provide CO with the document so that identified responsibilities can be reflected in the SLAs or contracts. |
| **Service Performance** | Identify Service performance measures with all responsible parties including those that are responsible for measuring performance. These should include capacity and capability of the CSO, elasticity, service monitoring, exception criteria, response time  
Additional system quality measures for service performance include accuracy, portability, interoperability, standards compliance, reliability, scalability, agility, fault tolerance, serviceability, usability, durability, etc. |
| **Service Reliability** | How Service reliability measures with all responsible parties are performed differs between IaaS, PaaS and SaaS services provided.  
As appropriate to the cloud service model, specify requirements for service resilience, preservation, protection, and secure back up of all audit trails and transaction logs of the system/network operations  
For SaaS providers, specify requirements for continuity of operations, and management of outages |
### Requirements to be incorporated in SLAs

<table>
<thead>
<tr>
<th>DESCRIPTION</th>
<th>Requirements to be incorporated in SLAs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attestation, Certification, &amp; Audits</td>
<td>Identify attestation and certification requirements to include FedRAMP Authorizations, DoD PA, and all requirements to comply with DoD policies</td>
</tr>
</tbody>
</table>
| Exit Strategy                  | Identify exit details/procedures for ensuring continuity with minimal disruption in the case of exit/termination of service when catastrophe or failure to perform/early termination, or completion of contract occur to include:  
  • The level of Contractor assistance in the exit process and any associated fees  
  • How and when the DoD data and networks will transition back to the DoD  
  • How the data will be transmitted and completely removed from the Contractor's environment once the exit process is complete. |
| Penalties                       | Identify a range of enforceable penalties and remedies, such as termination, for non-compliance with SLA performance measures. These penalties may be already included in FAR and DFAR standard clauses (i.e., Charge back approaches for unexcused performance failures) |

### CH 6–3.10 Protecting Information Technology

The Department released its [Cybersecurity Strategy](#) on April 17, 2015. It identifies the DoD's three primary cyber missions.

- The DoD must defend its own networks, systems, and information
- DoD must be prepared to defend the United States and its interests against cyberattacks of significant consequence.
- Third, if directed by the President or the Secretary of Defense, DoD must be able to provide integrated cyber capabilities to support military operations and contingency plans.

The DoD’s networks and systems are vulnerable to intrusions and attacks, and it is critical to develop and implement strong cybersecurity and program protection strategies and plans.

### CH 6–3.10.1 Cybersecurity

Cybersecurity risk management tasks should begin early in the system development life cycle and are important in shaping the security capabilities of the system. If not effectively performed early, the tasks, undertaken later in the lifecycle, will be more costly and time consuming to implement, and could negatively impact the performance of the system and its overall cybersecurity.

There are two general categories of cybersecurity operations – defensive and offensive.

- Defensive Cybersecurity. The protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.
- Offensive Cyber Operations. Joint Publication 3-12 (R) defines Offensive Cyberspace Operations as “Cyberspace operations intended to project power by the application of force in or through cyberspace. However, for SNaP-IT and OMB taxonomy purpose, Offensive Cyberspace Operations are activities that actively gather information, manipulate, disrupt, deny, degrade, or destroy adversary computer information systems, information, or networks through cyberspace.

All acquisitions of systems containing IT, including NSS, must produce a Cybersecurity Strategy. Beginning at Milestone A, PMs will submit the Cybersecurity Strategy to the cognizant CIO for review and approval prior to milestone decisions or RFP release per Enclosure 1, Table 2 of the DoDI 5000.02. The Cybersecurity Strategy is attached as an appendix to the Program Protection Plan (PPP) for submittal. More information on the Cybersecurity Strategy is located in [CH 8 Section 3.5.7](#).
CH 6–3.10.1.1 Responsibility
Cybersecurity is both a functional and acquisition responsibility due to its criticality. Both PMs and Functional Sponsors or Managers should be familiar with statutory and regulatory requirements governing cybersecurity, and understand the major tasks involved in developing an cybersecurity organization, defining cybersecurity requirements, incorporating cybersecurity in a program's architecture, developing a Cybersecurity Strategy, conducting appropriate cybersecurity testing, and achieving cybersecurity certification and accreditation for the program.

DoD recently revised several of its policies to more explicitly address the integration of cybersecurity into acquisition processes:

- Department of Defense Instruction (DoDI) 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), March 12, 2014; cancels the previous DoD Information Assurance Certification and Accreditation Process (DIACAP) and institutes a new, risk-based approach to cybersecurity through the Risk Management Framework
- DoDI 5000.02, Operation of the Defense Acquisition System, January 7, 2015; includes regulatory cybersecurity requirements such as the Cybersecurity Strategy artifact and risk management activities involving Authorizing Officials (AO)
- DoDI 8500.01, Cybersecurity, March 14, 2014; establishes that cybersecurity must be fully integrated into system life cycles

CH 6–3.10.2 Program Protection Planning
For the acquisition of software-intensive IT, especially IT used in National Security Systems, PMs should consider the significant operational threat posed by the intentional or inadvertent insertion of malicious code. The risks associated with these supply chain risk management (SCRM) issues are being managed within the context of program protection planning. CH 9 Section 2.3 regarding Program Protection Plan requirements as well as key practices and intelligence support from the Defense Intelligence Agency SCRM Treat Assessment Center (TAC).

For IT systems, areas of particular interest are protection and assurance activities undertaken during the integration and development of commercial off-the-shelf (COTS) components activities designed to mitigate attacks against the operational system (the fielded system); and activities that address threats to the development environment.

Additional information on program protection planning is provided in:

- The template and guide for the Program Protection Plan
- Guidance on Software Assurance Countermeasures
- CH 9 Section 2.2 Program Protection Policy and Guidance

CH 6–3.10.3 Risk Management Framework for IT
The RMF informs the entire acquisition process, beginning with requirements development and programs should be converting from the DoD Information Assurance Certification and Accreditation Process (DIACAP). A DIACAP and RMF knowledge portal (CAC required) is available in addition to a number of other resources:

- RMF Training Documents, April 4, 2014
- RMF Implementation, April 4, 2014
- Cybersecurity and RMF Implementation Training Video, May 8, 2014
- Program Manager’s Guidebook for Integrating the Cybersecurity RMF into the System Lifecycle, September 2015
- CH 9 Section 3.2.2 Risk Management Framework for DoD IT
While the RMF and requirements and acquisition hierarchies are distinct, they share a common baseline of security system engineering documentation and coordination among decision authorities. Engagement between the cybersecurity and acquisition communities is critical to management of cybersecurity-related risks to system performance.

**CH 6–3.10.3.1 Categorizing Information Technology for Security**

DoD Instruction 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT) Enclosure 6 establishes the process to categorize IT, select security controls, implement those controls, assess the controls, achieve authorization of the system and monitor the security controls. In the categorization process, the PMs/ISO identifies the potential impact (low, moderate, or high) resulting from loss of confidentiality, integrity, and availability if a security breach occurs. For acquisition programs, this categorization will be documented as a required capability in the initial capabilities document, the capability development document, the capabilities production document, and the cybersecurity strategy within the program protection plan (PPP).

**CH 6–3.11 Test and Evaluation for Information Technology**

On September 14, 2010, the Director, Operational Test and Evaluation, signed a memorandum entitled "Guidelines for Conducting Operational Test and Evaluation of Information and Business Systems." The guidelines help streamline and simplify COTS software testing procedures. They assist in tailoring pre-deployment test events to the operational risk of a specific system increment acquired under OSD oversight. For increments that are of insignificant to moderate risk, these guidelines streamline the operational test and evaluation process by potentially reducing the degree of testing. Simple questions characterize the risk and environment upon which to base test decisions, for example, "If the increment is primarily COTS, or government off-the-shelf items, what is the past performance and reliability?"

CH 8 describes various testing policies and practices.

**CH 6–3.11.1 Prototyping and Piloting**

Risk reduction prototypes will be included if they will materially reduce engineering and manufacturing development risk at an acceptable cost. Risk reduction prototypes can be at the system level or can focus on sub-systems or components.

The OSD office of Emerging Capability and Prototyping may be able to assist in guiding your prototyping activities.

- *Proof-of-principle prototyping* validates the technical feasibility of a capability and explores its operational value.
- *Pre-engineering and manufacturing development prototyping* advances capabilities that have already demonstrated some technical and operational promise.

Typically this type of activity is done on items that are not COTS; however, prototyping and piloting may still hold value in a tailored manner for information technology in the risk reduction phase in order to see real-time application of technology to down-select.

**CH 6–3.11.2 Developmental Testing**

Developmental Test & Evaluation (DT&E) is used to verify that the system under test meets all technical requirements. MDAP and MAIS ACAT I and IA programs are supported by a chief developmental tester and a governmental test agency that serves as the lead DT&E organization. The PM, who is ultimately responsible for all aspects of system development, selects a Chief Developmental Tester. The Chief Developmental Tester is a highly experienced T&E professional, authorized by the PM to conduct all duties in the area of T&E for the program. Inputs from the Chief Developmental Tester to the contract, engineering specifications, systems engineering efforts, budget, program schedule, etc., are essential if the PM is to manage T&E aspects of the program efficiently.

For IT programs, one of the most critical aspects of developmental test is to ensure an operationally-representative DT environment.
Additional guidance on developmental testing is available in the DoDI 5000.02 Enclosure 4 as well as CH 4 Section 3.3.2.2.

**CH 6–3.11.3 Operational Testing**

The appropriate operational test organization will conduct operational testing in a realistic threat environment. The threat environment will be based on the program's System Threat Assessment Report and appropriate scenarios. For MDAPs, MAIS programs, and other programs on the DOT&E Oversight List, the DOT&E will provide a report providing the opinion of the DOT&E as to whether the program is operationally effective, suitable, and survivable before the MDA makes a decision to proceed beyond LRIP. For programs on the DOT&E Oversight List, operational testing will be conducted in accordance with the approved TEMP and operational test plan. The Department's independent operational test agencies likely have guides or other training available on how to conduct operational testing, especially tailored to Service requirements. The Air Force Operational Test and Evaluation Center (AFOTEC), for example, has a detailed operational test guide available. Additional guidance on operational testing is available in the DoDI 5000.02 Encl. 5 Sec 7 Enclosure 5 section 7 of DoDI 5000.02 as well as CH 8 Section 3.2.

**CH 6–3.11.4 Cybersecurity Test and Evaluation**

Per the DOT&E Cybersecurity T&E Guidebook, “Potential cyber vulnerabilities, when combined with a determined and capable threat, pose a significant security problem for the DoD and its warfighters. Cybersecurity test and evaluation (T&E) assists in the development and fielding of more secure, resilient systems to address this problem.” The Guidebook outlines steps for planning, analysis, and implementation of cybersecurity T&E. Fundamentally, cybersecurity T&E consists of iterative processes, starting at the initiation of an acquisition and continuing throughout the entire life cycle.

The critical piece of documentation is the Test and Evaluation Master Plan (TEMP). The RMF may also drive cybersecurity testing requirements.

**Process**

Develop a strategy and budget resources for cybersecurity testing. The test program will include, as much as possible, activities to test and evaluate a system in a mission environment with a representative cyber-threat capability. CH 8 Section 3.2.4 discusses survivability and cybersecurity testing as well.

- Beginning at Milestone A, the TEMP will document a strategy and resources for cybersecurity T&E. At a minimum, software in all systems will be assessed for vulnerabilities. Mission critical systems or mission critical functions and components will also require penetration testing from an emulated threat in an operationally realistic environment during OT&E.
- Beginning at Milestone B, appropriate measures will be included in the TEMP and used to evaluate operational capability to protect, detect, react, and restore to sustain continuity of operation. The TEMP will document the threats to be used, which should be selected based on the best current information available from the intelligence community.
- The Program Manager, T&E subject matter experts, and applicable certification stakeholders will assist the user in writing testable measures for cybersecurity and interoperability.
- The Program Manager and Operational Test Authority will conduct periodic cybersecurity risk assessments to determine the appropriate Blue/Green/Red Team, and operational impact test events in alignment with the overall test strategy for evaluating the program for real world effects. Defense business systems will undergo Theft/Fraud operational impact testing.

**CH 6–3.12 Sustaining Information Technology**

**CH 6–3.12.1 Post Implementation Reviews**

The requirement for a PIR is outlined in the DoDI 5000.02 Enclosures 11 of DoDI 5000.02 (Page 120) and is directed by Title 40 U.S.C. section 11313.

The Functional Sponsor, in coordination with the Component CIO and Program Manager, is responsible for developing a plan and conducting a PIR for all fully deployed IT, including NSS. PIRs are intended
report the degree to which DOTMLPF-P changes have achieved the established measures of effectiveness for the desired capability; evaluate systems to ensure positive return on investment and decide whether continuation, modification, or termination of the systems is necessary to meet mission requirements; and document lessons learned from the PIR. If the PIR overlaps with Follow-on Operational Test and Evaluation, the sponsor should coordinate planning of both events for efficiency.

The basic high-level process for conducting a PIR is:

- Plan for the PIR and document in a PIR Plan
- Conduct the PIR, ensuring discussion of items such as ROI, measures met / not met, lessons learned, benefits achieved, etc.
- Conduct analysis based on the PIR findings
- Document the results in a PIR Report for feedback into the sustainment program

**CH 6–3.12.2 Operations and Sustainment of IT**

The purpose of O&S for IT is to execute the product support strategy, satisfy materiel readiness and operational support performance requirements, and sustain the system over its life cycle (to include disposal). The O&S Phase begins after the production or deployment decision and is based on an MDA-approved Lifecycle Sustainment Plan (LCSP). DoDI 5000.02 Encl 6 Enclosure 6 of DoDI 5000.02 includes a broader discussion of sustainment planning to include LCSPs and metrics. Sustainment planning is discussed throughout CH 4 beginning in Section 2.1. LCSPs are also discussed in CH 8 Section 3.5.12.

The phase has two major efforts, Sustainment and Disposal. The LCSP, prepared by the Program Manager and approved by the MDA, is the basis for the activities conducted during this phase.

**Sustainment**

During this phase, the Program Manager will deploy the product support package and monitor its performance according to the LCSP. The LCSP may include time-phased transitions between commercial, organic, and partnered product support providers. The Program Manager will ensure resources are programmed and necessary IP deliverables and associated license rights, tools, equipment, and facilities are acquired to support each of the levels of maintenance that will provide product support; and will establish necessary organic depot maintenance capability in compliance with statute and the LCSP.

**Disposal**

At the end of its useful life, a system will be demilitarized and disposed of in accordance with all legal and regulatory requirements and policy relating to safety (including explosives safety), security, and the environment.

**CH 6–3.12.3 Upgrades**

Upgrades on business capabilities and system occur on a relatively regular basis and throughout the lifecycle. This includes:

- Ongoing maintenance to correct existing processing, performance and implementation defects.
- Regular enhancements based on user feedback
- Preventive maintenance for software efficiency and to prevent corruption (e.g., anti-virus tools).
- Identification of new requirements or upgrades to improve performance, maintainability, and add functionality. If the changes are major in terms of cost, schedule, and or / performance, it may require the instantiation of a new program increment.

**CH 6–4. Additional Planning Considerations**

Additional best practices or other unique process requirements for the development and implementation of IT programs are discussed throughout this section.
CH 6–4.1 Best Practice and Lessons Learned

The following best practices for IT acquisition were originally introduced in 2010 through the Better Buying Power (BBP) initiative and built upon through successive BBP iterations. The principles of BBP apply to all acquisitions, and are being adopted through the IT acquisition community to improve affordability and delivery outcomes in IT acquisition. Many of the BBP principles that have translated throughout programs are:

- affordability constraints;
  - view resources: affordability
- should-cost management,
  - view resources: cost control
- elimination of unproductive processes and bureaucracy (i.e., tailoring);
  - view resources: eliminate unproductive processes
- strong incentives to industry,
  - view resources: incentives and communication with industry
- promoting competition,
  - view resources: promoting competition
- improving innovation, and product quality;
  - view resources: improving innovation
- In addition to
  - promoting technical excellence;
  - use of data to inform policy, and
  - a focus on cybersecurity to secure sensitive and classified data

Furthermore, the USD(AT&L) has solicited feedback from those individuals actually acquiring and implementing systems in the Department – and published it for others to read and learn from. For example, in 2015 the USD asked Program Managers of various ACAT I programs to submit assessments to him. With permission, he compiled some of them into a report which is available for viewing here. Taking this theme even a step further, the USD(AT&L) solicited feedback from Program Executive Officers (PEOs) regarding their portfolios and any suggestions they might have for improving results. Those results, which are mostly unedited, were published in the July-August 2016 Issue of DAU’s Defense AT&L Magazine.

Finally, the Government Accountability Office (GAO) has identified a set of essential and complementary management disciplines that provide a sound foundation for information technology (IT) management. These include: IT strategic planning, Enterprise architecture, IT investment management and Information Security; additional information is available through the GAO’s website on the issue summary.

CH 6–4.2 Root Cause Analysis

One of the issues the Department faces with successfully fielding IT capabilities is making the leap from problem to solution too quickly, resulting in a solution that doesn’t meet the fundamental need but rather provides temporary “band-aids” for its symptoms. The tendency to “do something now!” must be appropriately balanced with a process that mitigates the risk of fixing a symptom vs. its root cause(s). Root Cause Analysis is a structured approach to determining a problem’s causal factors and identifying what behaviors, actions, inactions, or conditions need to be changed in order to eliminate the problem.

There is no single methodology for performing Root Cause Analysis and various approaches can yield satisfactory results. Different approaches to identify potential root causes include:

- Affinity Diagram
- Fishbone Diagram
- Five Whys Analysis
- Pareto Diagram
- Value Analysis
Your Service / Component may have a specific preference toward root cause analysis methodology. The results of a root cause analysis will eventually lead to the definition of a requirement, which will be documented in a Problem Statement or an ICD, depending on the type of requirement.

**CH 6–4.3 General Management Practices for IT Programs**

The following are best practices for management of IT programs. Some are controllable at the individual Program Management level, while some are more strategic in nature and will require involvement of a PEO-type leader to ensure the right level of strategy and management oversight of a program:

- Ensure linkage to an IT strategic planning process, which typically occurs at the agency level (but may be derived and managed at lower levels in an agency or Service).
- Document a process to integrate IT management operations and decisions with organizational planning, budget, financial management, human resources management, and program decisions.
- Require that cyber security management processes be integrated with strategic and operational planning processes.
- Institute a process to account for all IT-related expenses and results.
- Prepare an enterprise wide strategic information resources management plan. At a minimum, an information resources management plan should (1) describe how IT activities will be used to help accomplish agency missions and operations, including related resources; and (2) identify a major IT acquisition program(s) or any phase or increment of that program that has significantly deviated from cost, performance, or schedule goals established for the program.
- Ensure its performance plan required under the Government Performance and Results Act of 1993 (GPRA), as amended by the GPRA Modernization Act of 2010 (1) describes how IT supports strategic and program goals; (2) identifies the resources and time periods required to implement the information security program plan required by FISMA; and (3) describes major IT acquisitions contained in the capital asset plan that will bear significantly on the achievement of a performance goal.
- Have a documented process to (1) develop IT goals in support of agency needs; (2) measure progress against these goals; and (3) assign roles and responsibilities for achieving these goals.
- Establish goals that, at a minimum, address how IT contributes to (1) program productivity, (2) efficiency, (3) effectiveness, and (4) service delivery to the public (if applicable).
- Establish IT performance measures to monitor actual-versus-expected performance. Measures should align with the GPRA performance plan.
- In an annual report, to be included in the budget submission, describe progress in using IT to improve the efficiency and effectiveness of agency operations and, as appropriate, deliver services to the public.
- Benchmark IT management processes against appropriate public and private sector organizations and/or processes in terms of costs, speed, productivity, and quality of outputs and outcomes.

**CH 6–4.3.1 Risk Management and Mitigation**

Successful risk management requires thoughtful planning and resourcing, and should be implemented as early as possible in the life cycle beginning with the Materiel Solution Analysis phase. The goal is to identify risks to inform decisions and handling strategies before the risks become issues. DAU has a risk management course available for basic training as well.

Risk management needs to be both top-down (embraced by the PM and others) and bottom-up (from working-level engineers) to be successful. PMs should encourage everyone on their program to take ownership of the risk management program and should be careful not to cultivate a “shoot the messenger” culture. All personnel should be encouraged to identify risks, issues, and opportunities and, as appropriate, to support analysis, handling, and monitoring activities.

Organizational implementation and process quality are equally important in determining a program’s risk management effectiveness. A poorly implemented risk management process will not contribute to program success and may lead to program inefficiency. It is essential that programs define, implement,
and document an appropriate risk management approach that is organized, comprehensive, and iterative, by addressing the following questions:

1. Risk Planning: What is the program’s risk management process?
2. Risk Identification: What can go wrong?
3. Risk Analysis: What are the likelihood and consequence of the risk?
4. Risk Handling: Should the risk be accepted, avoided, transferred, or mitigated?
5. Risk Monitoring: How has the risk changed?

**Figure 7: Risk Management Process**

<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DITPR</td>
<td>The unclassified authoritative inventory of IT systems. It contains information on DoD’s mission critical and mission essential information technology systems and their interfaces including the following: system names, acronyms, descriptions, sponsoring component, approval authority, points of contact, and other basic information. The information stored in DITPR provides DoD decision makers an overarching view of DoD’s IT capabilities for making resource decisions. It is the responsibility of the Program Manager (PM) to ensure that IT is registered and follows all applicable DoD Component Chief Information Officer (CIO) procedures and guidance. Additional information about DITPR can be accessed from here. DITPR can be accessed here. A DITPR account can be requested here.</td>
</tr>
<tr>
<td>Tool</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>DITIP</strong>&lt;br&gt;DoD Information Technology Investment Portal</td>
<td>DITIP provides a centralized location for IT investment portfolio data, is the authoritative data source for DoD IT Header information, and aligns IT systems information in the Defense IT Portfolio Registry (DITPR) with budget information in the Select and Native Programming Data Input System for IT (SNaP-IT). A DITIP account can be requested <a href="#">here</a>. For additional guidance on managing DBS using DITIP, access the DITIP website and select “DITIP Instructions – DBS Certification Management”.</td>
</tr>
<tr>
<td><strong>SNaP-IT</strong>&lt;br&gt;Select &amp; Native Programming Data Input System for Information Technology</td>
<td>SNaP-IT is the authoritative Department of Defense (DoD) database used for publishing the DoD Information Technology (IT) Budget Estimates to Congress, the Circular A-11 Section 53 and Section 300 exhibits to the Office of Management and Budget (OMB), and for monthly IT performance reporting to the IT Dashboard. You can access SNaP-IT guidance for these work products within the DoD Financial Management Regulation (7000.14-R, Volume 2B, Chapter 18) or within annual budget guidance issued by OUSD(C), D, CAPE, and DoD CIO. SNaP-IT can be accessed <a href="#">here</a>.</td>
</tr>
<tr>
<td><strong>PRCP</strong>&lt;br&gt;Program Resources Collection Process</td>
<td>DoD web-based application designed to prepare and manage direct program budget details. All MDAPs shall submit PBR data at the sub-program level and all MAIS programs shall submit at the Increment level as appropriate, consistent with the Track-to-Budget rules established for the data submission to PRCP, per the program/budget transparency requirements of the Fiscal Year Integrated Program/Budget Submission Guidance. PRCP is available on the SIPRnet.</td>
</tr>
<tr>
<td><strong>DAMIR</strong>&lt;br&gt;Defense Acquisition Management Information Retrieval</td>
<td>DAMIR provides enterprise visibility to Acquisition program information. DAMIR streamlines acquisition management and oversight by leveraging web services, authoritative data sources, data collection, and data repository capabilities. DAMIR identifies various data sources that the Acquisition community uses to manage Major Defense Acquisition Programs (MDAP) and Major Automated Information Systems (MAIS) programs and provides a unified web-based interface through which to present that information. DAMIR is the authoritative source for Selected Acquisition Reports (SAR), SAR Baseline, Acquisition Program Baselines (APB), MAIS Annual Reports (MAR), MAIS Original Estimates (MAIS OE), and Assessments. It is a powerful reporting and analysis tool with robust data checks, validation, standardization and workflow leveling. It has extensive security capabilities as well as both classified and unclassified versions. One component of DAMIR, Purview, is an executive information system that displays program information such as mission and description, cost &amp; funding, schedule, and performance. The DAMIR site, with directions for obtaining an account, can be accessed <a href="#">here</a>.</td>
</tr>
<tr>
<td><strong>AIR</strong>&lt;br&gt;Acquisition Information Repository</td>
<td>AIR is a searchable document repository for final milestone documents for Pre-Major Defense Acquisition Programs, Unbaselined Major Automated Information Systems, Acquisition Category (ACAT) ID, ACAT IAM, and Special Interest Programs. PMs are not responsible for uploading reports directly, but programmatic reports, such as an Analysis of Alternatives (AoA) or Clinger Cohen Act (CCA) compliance confirmation will be uploaded by the responsible agency. A list of these reports with the corresponding Office of Primary Responsibility (OPR), as well as the rationale behind AIR can be found at in the Acquisition Information Repository Implementation Guidance Memorandum signed by the USD(AT&amp;L) dated September 25, 2012. To access the AIR site, with directions for obtaining an account, go <a href="#">here</a>.</td>
</tr>
<tr>
<td><strong>DAT</strong>&lt;br&gt;DAE Action Tracker</td>
<td>DAT is a system that tracks action items from Acquisition Decision Memorandums (ADMs) and their status. The decisions and direction resulting from each acquisition milestone and other major decision point reviews are documented in an ADM. ADMs are ultimately signed by the MDA. The status of all ADM-directed actions for MAIS, MDAP, and Special Interest programs are tracked in DAT. As a PM it is important to pay close attention and work to quickly rectify any ADM actions because of their high visibility. DAT can be accessed <a href="#">here</a>.</td>
</tr>
</tbody>
</table>
### CH 6–4.5 Data Sharing Tools

This section addresses those tools, technology standards and specifications that are key enablers in driving data and information sharing. The section attempts to be comprehensive; yet, acknowledges the difficulty in keeping pace with rapidly evolving technologies. All of these enablers are recommended for use, as applicable. PMs should recognize that some are mandated in different policies and guidance documents and use as required.

The following table provides a brief description of some sample tools that can be used when implementing the sharing of data, information, and IT services.

<table>
<thead>
<tr>
<th>Tool</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Controls</td>
<td>Provides the mechanism to validate the rights or privileges (authorization) and claims of identity (authentication) for a user and matches those user credentials to defined access policies in order to make the grant or deny decision that is enforced through the policy enforcement point.</td>
</tr>
<tr>
<td>Adapter Services</td>
<td>Provides transformation or mediation of data assets and exchange formats. To be used for legacy system or data integration and federated domain transportation.</td>
</tr>
<tr>
<td>Cryptographic Binding</td>
<td>Creates a relationship between data objects and metadata tags by hashing the data object(s) and metadata and signing over the hashes with a signature using cryptography as a technique to ensure the integrity and authentication of data (i.e., no modifications, deletions or insertions by unauthorized sources).</td>
</tr>
<tr>
<td>Data Services Environment (DSE)</td>
<td>Provides an on-line repository enabling developers to reuse, understand, and share existing data assets. It addresses structural and semantic metadata such as schemas, web service description language, stylesheets, and taxonomies; descriptive metadata about proposed and approved ADSs, including their relationships and their responsible governance authorities; and descriptive, semantic, and structural metadata about services and other functional capabilities, including service definitions and specifications that can be discovered for subsequent use.</td>
</tr>
<tr>
<td>Data Tagging User Interface (UI)</td>
<td>Adds metadata tags to a data asset on the backend via a general Web UI, portal or local tagging tool. It is primarily used in a thin client or cloud environment.</td>
</tr>
<tr>
<td>Tool</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DoD Information Technology (IT) Standards Registry (DISR)</td>
<td>The DISR is an online repository of IT standards. It defines the service areas, interfaces, standards (registry elements), and standards profiles applicable to all DoD systems. Use of the registry is mandated for the development and acquisition of new or modified fielded IT systems throughout the DoD.</td>
</tr>
<tr>
<td>DoD Storefront</td>
<td>Provides an access point for end-users to discover data assets.</td>
</tr>
<tr>
<td>Enterprise Authoritative Data Source (EADS)</td>
<td>Provides a registry of DoD data needs, data sources authoritative bodies (ABs) and AB-approved assertions on the context upon which a given data source is authoritative. EADS is part of the Data Services Environment (DSE).</td>
</tr>
<tr>
<td>Enterprise Catalog</td>
<td>Provides a repository for data providers to publish DDMS-compliant discovery metacards.</td>
</tr>
<tr>
<td>Enhanced Information Support Plan (EISP)</td>
<td>The Enhanced Information Support Plan (EISP) tool is used to fulfill the requirements for creating an ISP. For more information, see section 7.3.6 of this Guidebook.</td>
</tr>
<tr>
<td>Enterprise Messaging</td>
<td>Allows applications to publish and receive information such as special reports, alerts, briefs or section-specific information over specialized logical messaging channels.</td>
</tr>
<tr>
<td>Federated Search</td>
<td>Provides the ability to find information across multiple sources without guesswork to use as part of Content Discovery. No special expertise in a complex query language or interface is required.</td>
</tr>
<tr>
<td>Forge.mil</td>
<td>Enables the collaborative development and use of open source and DoD community source software.</td>
</tr>
<tr>
<td>Global Information Grid (GIG) Technical Guidance – Federation (GTG-F)</td>
<td>The GTG-F is a suite of software applications that provides technical guidance. The GTG-F content consists of and is based on GIG net-centric IT standards, associated profiles, engineering best practices and reference implementation specifications.</td>
</tr>
<tr>
<td>Metadata Registry (MDR)</td>
<td>Collects, stores, and disseminates structural and semantic metadata artifacts critical to successful development, operation and maintenance of existing and future DoD capabilities. MDR is part of the DSE.</td>
</tr>
<tr>
<td>Metadata Tagging Tools (e.g., AMTT)</td>
<td>Tools that extract information from data assets in order to generate metacards or documents with imbedded metadata.</td>
</tr>
<tr>
<td>Net-Centric Publisher (NCP)</td>
<td>Automatically publishes data assets to the Metadata Registry, Service Registry and Enterprise Catalog. NCP is part of the DSE.</td>
</tr>
<tr>
<td>Search Widgets and Applications</td>
<td>Leverages services for search and discovery of metadata cards and assets for various widgets and applications, primarily during the development and design phases.</td>
</tr>
<tr>
<td>Secure Data Tagging Tool (SDTT) Suite</td>
<td>NSA data tagging toolset. It includes reusable components that allow analysts and stakeholders to create metadata tags, validate them for conformance and reasonability to Controlled Access Program Coordination Office (CAPCO) or other standards, and perform cryptographic binding of the metadata to the data asset(s).</td>
</tr>
<tr>
<td>Security Mechanisms</td>
<td>Provides security implementations, configurations and protocols aimed at mitigating or stopping security threats throughout the enterprise. Includes mechanisms such as IdAM, XML Gateways, PKI, etc.</td>
</tr>
</tbody>
</table>
## Tool and Purpose

<table>
<thead>
<tr>
<th>Tool</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Discovery (SD)</td>
<td>Searches the Enterprise Service Registry for service providers and services. SD is part of the DSE.</td>
</tr>
<tr>
<td>Service Registry (SR) (Universal Description Discovery and Integration [UDDI])</td>
<td>Provides the information required for an application developer to locate an appropriate service, determine the features and functions provided by that service, identify how to invoke the service, and determine where the service resides.</td>
</tr>
<tr>
<td>Smart Data</td>
<td>Tags all the data so users can track it, know the sensitivity, and apply access control values, provenance and smart routing.</td>
</tr>
<tr>
<td>Transport Protocols</td>
<td>Provide a standardized means for routing and transportation across a net-centric environment. Can be any of the technical protocols used for transportation and routing such as Hyper Text Protocol (HTTP), SOAP/HTTP, SOAP/Java Message Service (JMS), FTP, etc.</td>
</tr>
<tr>
<td>User Authentication and Authorization Services</td>
<td>Provides dynamic and account based access control to support the automated provision of web services and attribute-based access to data and resources using policy decision points and policy enforcement points. This is the foundation for access control throughout the Joint Information Environment (JIE).</td>
</tr>
</tbody>
</table>

## CH 6–Version and Revision History

The table below tracks chapter changes. It indicates the current version number and date published, and provides a brief description of the content.

<table>
<thead>
<tr>
<th>Version #</th>
<th>Revision Date</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>11/2/16</td>
<td>Chapter 6 initial upload</td>
</tr>
<tr>
<td>0</td>
<td>02/01/17</td>
<td>CH 6–3.9.2 Cloud Computing – links validation</td>
</tr>
<tr>
<td>0</td>
<td>9/29/17</td>
<td>Links validation for all sections</td>
</tr>
</tbody>
</table>