UMD-AM-12-173

IT Acquisition: Expediting the Process to Deliver Business Capabilities to the DoD Enterprise

By:

Jacques S. Gansler and William Lucyshyn

Center for Public Policy and Private Enterprise
School of Public Policy

Revised July 2012

This research was partially sponsored by a grant from
The Naval Postgraduate School

The Center for Public Policy and Private Enterprise provides the strategic linkage between the public and private sector to develop and improve solutions to increasingly complex problems associated with the delivery of public services—a responsibility increasingly shared by both sectors. Operating at the nexus of public and private interests, the Center researches, develops, and promotes best practices; develops policy recommendations; and strives to influence senior decision-makers toward improved government and industry results.

Table of Contents

Executive Summary

Information technology (IT) offers inestimable capability and has been leveraged extensively by the Department of Defense (DoD) to build national security systems, business systems, and virtually all of today's weapon systems. As the DoD continues to transform its forces and business systems to meet the challenges of the 21st century, it will continue to rely on the increased functionality that IT delivers, even as its cost decreases.

The DoD's goal is to acquire IT systems quickly and cost effectively. However, this goal is rarely achieved because the deliberate process through which the DoD acquires IT systems does not—and cannot—keep pace with the rapid development that is occurring in today's information age. The DoD relies upon a singular, one-size-fits-all process to acquire its systems and services. As a result, IT systems are subject to excessive risk-reduction strategies, suboptimal test and evaluation (T&E) protocols, and inflexible requirements. Improving the acquisition process for IT is critical if the DoD is to reduce costs and improve the effectiveness of its systems.

The DoD has made several revisions to its acquisition policies in an attempt to shorten the acquisition cycle-time. These revisions, however, consist of little more than changes to the traditional acquisition model. Unsurprisingly, these reform initiatives have generally not had much impact—the time line for IT acquisitions remains incredibly long. A 2010 House Armed Services Committee (HASC) Panel on Defense Acquisition Reform found that the delivery of defense IT systems requires between 48 and 60 months. Considering that commercial IT is on a 12- to 18-month upgrade cycle, it is often the case that the DoD's new IT systems are outdated—often by several generations—by the time they are implemented.

A successful IT project is often defined as one that is delivered on time and on budget, with the required features and functions (The Standish Group, 1995).). The project should also be of the current IT product generation (i.e., the product in question should be contemporaneous with commercially available systems, or in the case of highly-specific DoD systems, the relevant technical elements of commercial systems). Studies of both commercial and government IT projects indicate that success is rarely achieved. For example, a 2008 Government

Accountability Office (GAO) report found that nearly half of all major federal government IT projects were re-baselined, with half of those being re-baselined more than once. Ideally, IT development would make use of a shorter time line, using an iterative process that regularly delivers updated products.

Multiple independent studies of the government's IT acquisition process have been undertaken in the last few years in an effort to identify ways to improve its overall effectiveness, and although some have focused directly on the DoD's IT acquisition, others have sought to address the more general, government-wide challenges. We conducted a meta-analysis of these and identified common threads with regard to process deficiencies and recommendations. Our proposed new acquisition process recognizes and adapts these commonly identified elements, attempting to correct the acknowledged deficiencies.

In 2010 Congress mandated that the Secretary of Defense implement a new IT acquisition process based on a 2009 Defense Science Board (DSB) Task Force report. Congress further stipulated that the system "be designed to include (1) early and continual involvement of the user; (2) multiple, rapidly executed increments or releases of capability; (3) early, successive prototyping to support an evolutionary approach; and (4) a modular, open-systems approach" (National Defense Authorization Act [NDAA], 2010, § 804). Our proposed acquisition process meets this mandate.

Our proposed process is specifically tailored to the unique, desired attributes of modern defense business systems. The process incentivizes the use of commercial off-the-shelf (COTS) products, encourages the development of enterprise solutions, and emphasizes technology-neutral approaches. Its conceptual goal is to complete one development cycle (360 degrees) in one year (approximately 360 days). Hence, it was named *IT 360*.[1] Embedded within *IT360* are a series of initiatives that, we believe, will allow the DoD to enhance the speed and efficiency with which it acquires its defense business systems. These initiatives include spiral development; smaller,

[1] The term *IT 360* was first used by Mr. Keith Seaman, the former Business Transformation Agency Component Acquisition Executive.

quicker to deliver, useful sets of capabilities; rapid delivery; the greater use of COTS products; the aggressive use of prototypes and demonstrations; continuous and integrated testing; decentralized execution; the inclusion of end users; and enhanced competition.

IT 360 is both an evolutionary and an incremental approach to IT acquisition. Indeed, the initial *IT 360* product iteration may not possess all of the desired capabilities. However, once the base architecture of the IT system in question is established, the process adds functionality to the system's existing capabilities at a standardized, quick pace. The *IT 360* process consists of seven phases that interact in a spiral fashion: (1) Program Initiation; (2) Increment Requirement Identification; (3) Initial Increment Level Material Development Strategy; (4) Architectural Alignment and Development; (5) Development, Demonstration, and Oversight; (6) Increment Capability Delivery; and (7) Operations and Maintenance.

To maximize the benefits of the *IT 360* acquisition process, we have identified four supporting initiatives: (1) documentation streamlining, (2) flexible contracting, (3) tailored program financial management, and (4) forward-looking standards and technology neutrality.

We have also outlined a multi-tiered governance structure for the new process that is designed to promote stakeholder integration, speed, and ease of access. Unlike the traditional acquisition system, whereby the majority of oversight takes place prior to milestones and during key decision points within a specific program or portfolio of programs; the *IT 360* process integrates oversight into each phase. In fact, one of the primary goals of the governance structure is maximizing internal adjudication—management personnel working directly within programs are in the best position to make qualified decisions.

The *IT 360* process has the potential to transform the DoD's approach to IT acquisition. However, for this transformation to take place, a number of specific challenges must be overcome. These challenges are outlined as follows:

- Contracting practices do not provide programs with enough contract flexibility at the portfolio level (across programs).

- Programs with evolving requirements are unduly constrained and unable to meet their full potential because the budgets of most DoD projects are established prior to its inception.
- The DoD does not fully engage industry partners, making it difficult to control costs in the face of the fluid, evolving requirements envisioned by *IT 360*.
- The DoD does not adequately balance the need for competition with contractor incentives.
- The DoD has yet to engage in an enterprise-wide expansion of security standards and protocols.
- The DoD lacks a disciplined approach with regard to the premature inclusion of system requirements.
- Procurement laws, regulations, policies, and processes are not tailored to the current defense acquisition system.
- The DoD lacks an appropriately trained, educated, and experienced acquisition workforce.

There are also a number of institutional barriers that must be removed in order for *IT 360* to be fully successful.

- The National Defense Authorization Act (NDAA, 2010) continues to require that all research and development (R&D) funds used for programs be submitted to Congress at the start of the program.
- Because defense business system programs often meet Major Automated Information Systems (MAIS) cost thresholds and are thus classified as such, defense business systems acquired via *IT 360* may be subject to the rigid MAIS reporting process.

- Congress designates different authorities to oversee the discrete processes embedded within the traditional acquisition system; under *IT 360*, these processes are largely obsolete and create oversight ambiguities.

- Congress requires that funds be used only for the programs and purposes for which the appropriation in question was made, rendering portfolio-level funding impermissible. To eliminate the ambiguity, funding should be through appropriations at the portfolio-level (mission area) for IT programs.

Milestone Decision Authorities currently have the flexibility to implement and use our proposed process with Acquisition Category (ACAT) III programs immediately. Once the challenges and barriers previously outlined are mitigated, *IT 360* can be extended to larger IT programs. We believe that this new process, in conjunction with the complementary governance structure and supporting initiatives, will facilitate the timely acquisition of effective defense business systems at lower cost, and with less risk.

I. Introduction

The Department of Defense (DoD) is the largest organization in the world, with operations that span a broad range of agencies, activities, and commands. With an annual budget approaching $700 billion in fiscal year (FY) 2012, the DoD employs millions of people that operate worldwide and maintains an inventory system that is an order of magnitude larger than any other in the world. However, the business systems used to manage these resources are outdated and inefficient, even as continual innovation in IT has made computing and networking cheaper and faster. These innovations have enabled many firms in the private sector to implement enterprise-wide systems, significantly improving productivity and efficiency.

More recently, IT has been used for far more advanced applications in virtually all types of organizations. Today, companies and government agencies are applying networked IT to facilitate complex tasks such as enterprise resource planning and supply chain integration. But although many private-sector firms (e.g., FedEx, Wal-Mart, Amazon) have successfully undergone a fundamental transformation of their businesses, government agencies have had much less success.[2] The DoD has not been able to successfully leverage the full potential productivity improvements that IT systems offer, and it still lags far behind the capabilities of the "world-class" private sector. This shortfall is, in large part, due to inefficiencies introduced by the DoD's acquisition process. Today, the DoD continues to rely on many non-integrated, non-interoperable legacy systems that are error-prone and redundant and that do not provide the enterprise visibility necessary to make sound management decisions.[3]

The DoD's one-size-fits-all acquisition process has, in many cases, failed to produce the required IT systems in a timely manner and within budget. Indeed, nearly half of all major federal IT projects undertaken have experienced delays or changes to requirements that have led to cost and schedule overruns and program restructuring. Of the re-baselined projects, half have

[2] The commercial sector has also experienced challenges—only 16% of commercial IT projects are completed on time and on budget, and 31% are cancelled prior to their completion (House Armed Services Committee [HASC], 2010).
[3] The DoD has reported that it relies on about 2,080 business systems, including accounting, acquisition, logistics, and personnel systems (Government Accountability Office [GAO], 2010).

encountered additional challenges and have been re-baselined at least one additional time (GAO, 2008). A 2010 House Armed Services Committee (HASC) Panel on Defense Acquisition Reform found that the delivery of defense IT systems requires between 48 and 60 months, and the former Deputy Secretary of Defense, William J. Lynn III, stated that the implementation of new IT systems takes an average of 81 months (Jackson, 2011). Considering that commercial IT systems are on a 12- to 18-month upgrade cycle, it is often the case that the DoD's new IT systems are outdated—often by several generations—by the time they are fully operational.

Recognizing this unacceptable trend, the DoD has introduced a number of initiatives in the last decade in an effort to improve IT acquisition. However, little progress has been made. Most stakeholders believe, as do we, that minor initiatives do not go far enough to address the underlying conditions and obstacles. We believe that a new IT-specific acquisition process is needed.

The current, linear process—contained in the DoD's 5000 Series publications—has proven relatively successful at producing effective weapons systems and platforms,[4] but the process is ill-suited to the acquisition of IT-centric systems, including the various types of defense business systems. For instance, because the 5000 Series process is used for all acquisitions, it incorporates higher levels of fiscal risk management in order to ensure that the most risk-prone types of procurements are pursued with caution. However, this level of risk management has proven excessive with regard to defense business systems, often delaying them beyond their effective time lines (Defense Science Board [DSB], 2009). Defense business systems must be developed at a faster rate in order to keep pace with new IT innovation. Failure to keep pace invites a different type of risk: premature program obsolescence.

We have developed a new process, *IT 360*, which, we believe, will enable the successful acquisition of defense business systems. *IT 360* encompasses four primary objectives:

[4] The initial version of the 5000 Series was first written in 1971 and has been updated several times (although the basic process has remained relatively unchanged). This documentation describes in detail the method of conducting defense acquisition. The current versions are DoD Directive 5000.01 and DoD Instruction 5000.02 .

- provide practical capabilities to the DoD enterprise quickly and efficiently;
- incorporate commercial management practices in order to reduce overall risk;
- grant maximum flexibility to the Milestone Decision Authority (MDA) in order to reduce the reporting and administrative burden; and
- respond effectively to the end users' needs.

Although this new process will remove many of the obstacles currently hindering IT procurement, it will not remove all of them. Accordingly, we have identified a number of initiatives to support the *IT 360* process. These initiatives include document streamlining, the use of flexible contracting mechanisms, and the implementation of forward-looking, technology-neutral standards. We believe that once these initiatives are aligned and interwoven with *IT 360*, the DoD will have the tools it needs to develop, acquire, and field world-class defense business systems.

According to 10 U.S.C. 2222(j)(2), a defense business system is "an information system, other than a national security system, operated by, for, or on behalf of the DoD [that is] used to support business activities such as acquisition, financial management, logistics, strategic planning and budgeting, installations and environment, and human resource management."

Although the moniker of "business system" may leave one with the impression that these systems support only back-office operations, this is not the case. These systems can have a direct impact on warfighting capability in that all military operations are inherently dependent on the appropriate level of logistics support, and, consequently, the business systems that support logistics functions.

Defense business systems can be categorized by the extent to which they rely on commercial products and solutions. Generally, defense business systems that leverage commercial development to the greatest degree practical will prove to be the most effective and efficient. The different categories of defense business systems are described in the following subsections.

DoD-Unique Systems

When the user requirements cannot be met in part, or in their entirety, by an existing or modified commercial product, the DoD must develop its own unique applications. While this type of full development enables the DoD to obtain a system that fulfills its every requirement, it generally requires a longer time commitment for software development, maturation, and testing (Adams & Eslinger, 2004). Furthermore, because the product is not available on the commercial market, the development of any complementary updates will also need to be fully sponsored by the DoD. This is generally the least efficient way to acquire a defense business system.

Commercial off-the-Shelf

Commercial off-the-shelf (COTS) IT products do not require modification or integration of other components prior to implementation by the DoD. While not all of the DoD's needs can be met by adopting and adapting a full COTS solution, the benefits provided are significant. Most notably, the DoD can leverage the investment made in the private sector, significantly reducing development time, and the need for research and development (R&D; Adams & Eslinger, 2004). Additionally, these products are developed based on industry "best practices" and are also routinely updated by the developer for use in the private sector. Because COTS products are, by definition, "as-is" products, their integration into larger systems can be very complex and may require modification or the adaptation of requirements.

Modified COTS

Modified COTS products are commercial systems that are modified by the contractor to meet specific DoD requirements. Similar to COTS, development time and R&D are significantly reduced compared to one-of-a-kind DoD-developed systems. This method of procurement allows for the greatest degree of user customization and update options. To the maximum extent possible, the modifications required should be minimized by

adapting the "historic DoD practices" to the "best practices" built into the COTS products.

Integrated COTS

To meet unique DoD requirements, it is sometimes necessary to integrate both COTS systems and custom-developed systems into a larger system. Although similar to modified COTS, integration of COTS systems as components differs in that the former requires modification while the latter involves the use of COTS systems as components within the integrated system.

Software as a Service

Software as a service (SaaS) is a software delivery model whereby software is hosted centrally (today, the emphasis is on hosting via the Internet, or "the cloud"). The idea of SaaS has been endorsed by the White House, and it has begun to gain some traction within the DoD. The recently released Cloud Computing Strategy (February 2011) asserted that "The cloud computing model can significantly help agencies grappling with the need to provide highly reliable, innovative services quickly, despite resource constraints" (Kundra, 2011, p.7). The decision to apply a specific cloud-computing model must take into account user requirements; for instance, security is of the utmost importance.

Report Approach

In Part II of this report, we provide a background and overview of the current acquisition process used by the DoD. We then explain why it is ill-suited to the acquisition of IT. We address emerging factors—from security threats to declining defense budgets—that highlight the inadequacies of the current system. In Part III, we present a synthesis of government reports, academic papers, and proposed strategies aimed at reforming IT acquisition. In Part IV, we present our solution, *IT 360*, a new approach to IT acquisitions that is based, in large part, on our analysis of the documents summarized in Part III. Next, we discuss our supporting initiatives and provide an overview of the complementary governance structure. In Part V, we discuss the

challenges and barriers that must be overcome for the new process to succeed. Finally, in Part VI, we provide concluding remarks.

II. Background

The DoD's current acquisition process is often described as a simple construct that efficiently integrates three interdependent processes: requirements, budgets, and procurements. Each of these processes, it is said, works both independently and cooperatively to drive the program toward meeting its objectives.

The first of these—the product (or, alternatively, the system's requirements)—are defined by the Joint Capabilities Integration and Development System (JCIDS), which also provides the evaluation criteria for the acquisition program. Secondly, the Planning, Programming, Budgeting, and Execution (PPBE) process is used to allocate and manage the DoD's financial resources. The third process, the Defense Acquisition System, is the mechanism through which DoD products and systems are developed and acquired. This process is described in some detail in the next section. In theory, each of these processes should work together in a coordinated fashion to deliver, in an efficient and cost-effective manner, essential capabilities to the DoD. However, the deficiencies of this overall process, especially with regard to the acquisition of defense business systems, have been known for some time. The Deputy Secretary of Defense's *Defense Acquisition Performance Assessment Report* (Defense Acquisition Performance Assessment Panel, 2006) describes the acquisition process as a highly complex mechanism that is fragmented in its operation. According to the report, "the differences in the theory and practice of acquisition, divergent values among the acquisition community, and changes in the security environment have driven the requirements, acquisition and budget processes further apart and have inserted significant instability into the Acquisition System" (p. 3). Under the current system, attempts to accelerate IT development cycles to keep pace with technical innovation serve only to amplify this fragmentation (Defense Acquisition Performance Project Panel, 2006). It is no surprise, then, that improving IT acquisition has been a stated goal of the DoD for over a decade.

The Defense Acquisition System

The Defense Acquisition System (codified in DoD Directive 5000.01, with detailed implementation instructions contained in DoD Instruction 5000.02) is used to acquire DoD products and systems (see Figure 1). The system is designed to translate mission needs and detailed requirements into stable, affordable, and well-managed acquisition programs. Although this linear acquisition process has a heritage based on the development of hardware systems, it is intended to accommodate the needs of all DoD programs, including IT.

The Defense Acquisition System, updated in December 2008, consists of five life-cycle phases.

- **Materiel Solution Analysis.** The purpose of this phase is to assess the potential materiel solutions for a military need; to refine the initial system solution; and to create a strategy for acquiring the solution. At the end of this phase, the program reaches Milestone A, where a decision is made as to whether or not the program will advance to the next phase.
- **Technology Development.** During this phase, technologies are developed, matured, and tested in conjunction with the simultaneous refinement of user requirements. By the completion of this phase, the program must have mature technology, approved requirements, full funding, an acquisition strategy, and the acquisition program baseline. Additionally, the type of contract that will be used to acquire the system must be specified. The Milestone B decision authorizes entry into the next phase.
- **Engineering and Manufacturing.** The purpose of this phase is to develop and integrate the full system, make preparations for manufacturing, and demonstrate (through testing) that the system can function in a real-world environment. The decision at Milestone C authorizes low-rate initial production (LRIP) of the system.
- **Production and Deployment**. During this phase the system is produced, operationally tested, and deployed.
- **Operations and Support.** This is the final phase. Program personnel ensure that the system is sustained over its life cycle.

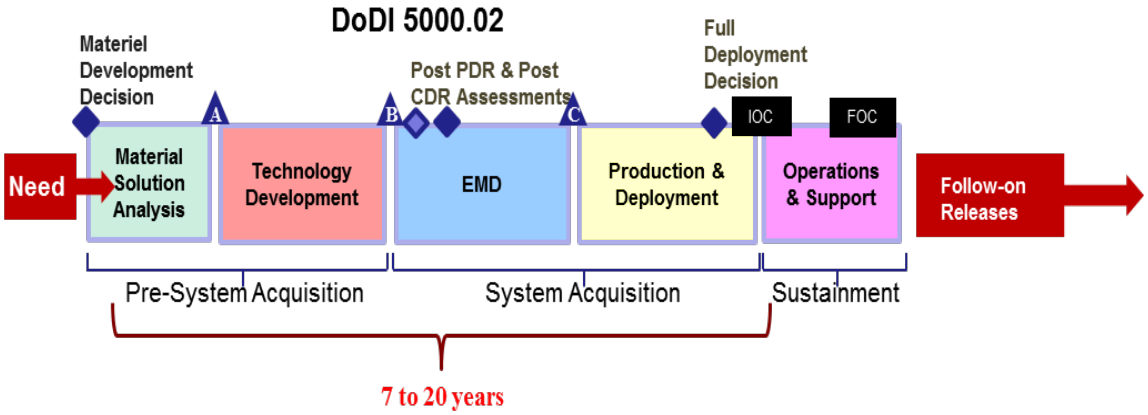

Figure 1. The Defense Acquisition System

(DoD, 2007)

Acquisition Categories and Designations

The DoD divides acquisition programs into four acquisition categories, or ACATs: ACAT I, ACAT IA, ACAT II, or ACAT III. ACAT I programs are those requiring the most significant investment. Non-IT programs estimated to require an eventual total expenditure of more than $365 million for research, development, test, and evaluation (RDT&E) or more than $2.190 billion for procurement[5] are designated as ACAT I. The most costly ACAT I programs are, in turn, designated as Major Defense Acquisition Programs (MDAPs). These require supplemental review, in addition to more programmatic evaluation and documentation.

Major Automated Information Systems (MAIS)

IT-based systems and services, on the other hand, can be designated as Major Automated Information Systems (MAIS). MAIS have their own thresholds and reporting requirements (see Figure 2). This process makes use of a shorter, five-year time line. While this time line

[5] Figures in this section are in FY2000 constant dollars.

represents an improvement over the traditional process, five years is still quite long within the context of IT, with projects transcending multiple generations of IT products.

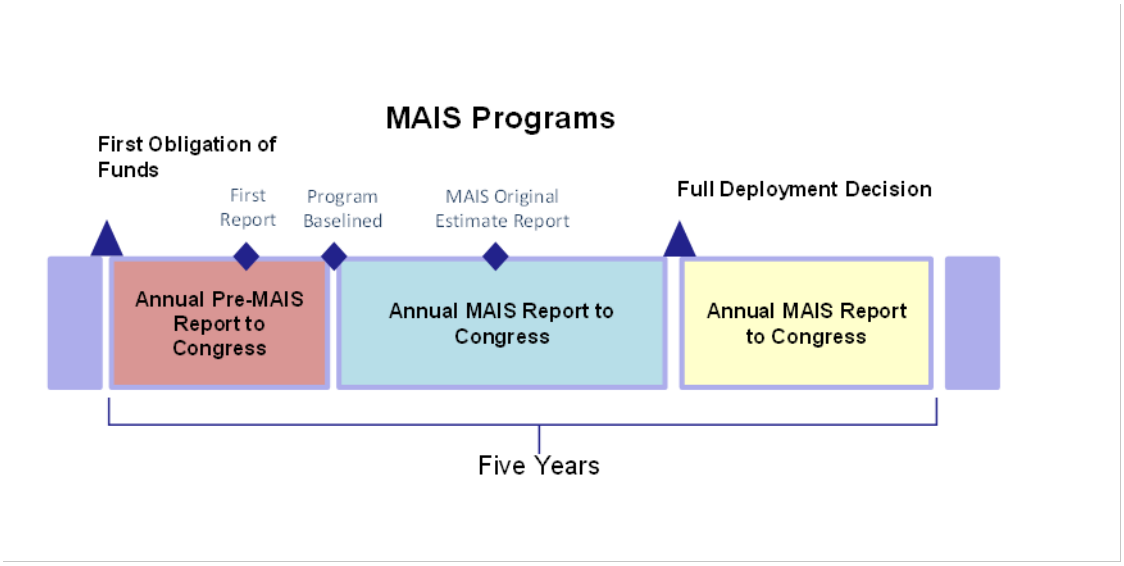

Figure 2. The Defense Acquisition Process for MAIS Programs

(DoD, 2007**)**

A DoD acquisition program for an Automated Information System (AIS) is categorized as an ACAT IA if it meets one of the following criteria:

- The program is designated by the MDA as a MAIS.
- The program is estimated to exceed $32 million (in FY2000 constant dollars) for all expenditures and for all increments, regardless of the appropriation or fund source, directly related to the AIS definition, design, development, and deployment, and incurred in any single fiscal year.
- The program is estimated to exceed $126 million (in FY2000 constant dollars) for all expenditures and for all increments, regardless of the appropriation or fund source, directly related to the AIS definition, design, development, and deployment, and incurred from the beginning of the Materiel Solution Analysis phase through deployment at all sites.

- The program is estimated to exceed $378 million (in FY2000 constant dollars) for all expenditures and for all increments, regardless of the appropriation or fund source, directly related to the AIS definition, design, development, deployment, operation, and maintenance, and incurred from the beginning of the Materiel Solution Analysis phase through sustainment for the estimated useful life of the system (DoD, 2007).

The Current Defense Acquisition Process Is Ill-Suited for IT

Some elements of the Defense Acquisition System only apply to weapons systems, some elements only apply to automated information systems, and some elements apply to both. The Defense Acquisition System has managed to successfully deliver weapons systems, and although they are often delayed and over budget, they generally prove to be very effective upon their deployment.

The average time frame of an acquisition program is 8–10 years; however, many programs have considerably longer durations. The F-22 program, for example, was delayed for more than ten years (in fact, more than 20 years passed between the start of development and initial operational capability). Defense IT programs tend not to take quite as long, but delays of long durations are still common. For instance, the Government Accountability Office (GAO) recently reported that six of the DoD's nine ACAT IC[6] Enterprise Resource Planning Systems experienced schedule delays ranging from 2 to 12 years, with development times ranging from 7 to 16 years (GAO, 2009). Most IT programs take between 48 and 60 months to deliver initial capabilities, with longer delivery times for MAIS programs. For 32 sampled MAIS programs, the average amount of time required to deliver an initial program capability was 91 months, or over 7 and a half years (Czelusniak, 1998).

Because the DoD's IT programs take so long to deliver, updating capabilities or requirements to incorporate new technologies can result in more delays and increased costs. Additionally,

[6] ACAT IC programs are MDAPs, for which the MDA is the DoD Component Head or, if delegated, the DoD Component Acquisition Executive (CAE). The letter *C* refers to *component* ("Component," 2011).

because the acquisition process does not allow for incremental delivery of capabilities, user feedback generally cannot be taken into account. Because user feedback is not incorporated into the current acquisition process, unnecessary functions are often built into new systems (Schwartz, 2009). The inclusion of these over-specified capabilities means that additional time is required to develop the system, thereby further delaying its release.

Indeed, IT acquisition has proved challenging not only for the DoD but also for commercial firms. For instance, even with commercial systems, over-specification is common. In a 2002 Standish Group report, 45% of commercial IT systems' designed functions were reported as never being used (Johnson, 2002). Only 16% of all IT projects (i.e., government and commercial) are completed on time and within budget, and 31% are canceled (HASC, 2010). The remaining 53% are late and over budget, with typical cost increases exceeding the original budget by more than 89% (HASC, 2010). Of the IT projects that are completed, the finished products contain only 61% of the originally-specified requirements (Johnson, 2002). Clearly, neither the DoD nor the commercial market are acquiring their IT products as efficiently as they could, and even if these figures reflect the true cost of acquiring IT (perhaps we simply underestimate the amount of time and money actually required to develop IT-based products), a more efficient acquisition process would reflect this reality through more accurate time lines and cost estimates.

One of the key differences between information systems and weapons systems is the pace of product evolution. With defense business systems, IT development and maturation occurs primarily in the commercial sector and is driven by customer demand and innovation; the DoD generally only plays a minor role. Commercial IT systems tend to evolve at an extremely rapid rate, with cycle-times approaching 18 months. As a result, delays to DoD IT programs of even one or two years can significantly reduce the potential utility of the system, and although risk reduction strategies and accountability controls are essential to the development of costly MDAPs, using the same approach with IT systems slows the timely delivery of effective information systems.

Moreover, many of today's IT products are modular (i.e., composed of standardized autonomous units allowing for flexible arrangement and reuse). As a result, the point at which Program X ends and Program Y begins is often not well defined with regard to IT systems. Rather, programs overlap, and transitions between systems (and transitions between components within systems), are interwoven to the point where the term *life cycle*—a mainstay of the traditional acquisition process—is increasingly meaningless within the context of IT acquisition.

Indeed, several of the phases of the Defense Acquisition System are of little relevance with regard to the development and deployment of information systems. For instance, LRIP has little meaning in the world of IT development; unlike tanks and aircraft, software programs are not produced on assembly lines. Incidentally, LRIP is one of the most risk-prone and most likely to be delayed phases of DoD programs (Cai et al., 2004). And while the serial T&E prior to production is essential to the development of weapons systems, IT development needs a continuous cycle of testing during the development. In fact, in the commercial market, software programmers often rely on a very short development process known as *test-driven development*, whereby the developer writes a failing automated test case that defines a desired improvement or new function, then produces code to pass that test, and finally re-factors the new code to acceptable standards (Beck, 2003).

Other Factors

Acquiring defense business systems using existing, outmoded processes is an increasing liability. Today, there are several other factors that are increasing the need for an improved IT acquisition process. These include (1) budgetary constraints, (2) poor performance, (3) rapid pace of technology, (4) private-sector dominance, and (5) security concerns.

1. Budgetary Constraints

> As the U.S. economy, still reeling from the recession of 2008, continues along the path to recovery, lawmakers are searching for ways to cut spending to reduce the country's $14.5 trillion debt. Congress has not yet developed a strategy to manage growing entitlement spending. Accordingly, the DoD, which consumes the second largest portion of

government revenue after entitlements, will likely see significant cuts in coming years. Indeed, cuts are already being made. In August 2011, Congress reached a budget deal that will impact the DoD budget in two ways. The first was a $350 billion cut in defense spending over the next 10 years. The second was the threat of some $600 billion more in cuts, which would be automatically triggered in January 2013 since a special congressional committee failed to agree on future deficit reductions. As top military leaders confront budgetary constraints, the DoD will have to address the process by which it provides services and acquires all of its systems.

2. Poor Outcomes

Information systems relying on the MAIS acquisition process have experienced significant challenges. Take, for instance, the case of the Defense Integrated Military Human Resource System (DIMHRS). In the late 1990s, the DoD's Business Transformation Agency launched the DIMHRS in an effort to consolidate more than 90 Service-unique military personnel and pay systems. The original acquisition cost estimate of approximately $6.5 million had increased to over $1 billion in 2008 (Gansler & Lucyshyn, 2009). The first phase of the DIMHRS—the consolidation of all payroll and personnel functions for the Army into one integrated web-based system—was expected to be completed in 2009. The other Services were expected to implement the system shortly thereafter. But following numerous delays, technical problems, and schedule setbacks, not to mention significant cost overruns, the DoD announced the program's cancellation in February 2010. Approximately $850 million had been spent (Kundra, 2010).

3. Rapid Pace of Technology

In 1965, Gordon Moore noted a trend in computing capabilities based on integrated circuits. First, he observed that the yields (as an increase in the number of components per function) in speed and power double every 18–24 months. Today, this is known as Moore's law of increasing yields. Since software is influenced to a large degree by

hardware capabilities, it is not surprising, then, that software capabilities change on the same timescale. Despite being first observed in 1965, this trend remains true today, as does its related impact on software. Since DoD IT systems currently take anywhere from 48 to 91 months to be developed, they are often outdated (or even obsolete) upon initial delivery, with some system elements several generations behind what is commercially available.

4. Private Sector Leads Innovation

IT innovation is driven, in large part, by the demand in the private market. Progressively more sophisticated versions of, say, the iPhone are released by Apple in response to near-continuous consumer demand. The accelerating rate at which new personal computers, smartphones, and MP3 players appear on store shelves is as much a function of new technology (creating the demand for new capabilities) as it is the accumulation by industry of users' feedback and desires. Once the two processes—user input and technological innovation—merge, an uninterrupted loop spurs ever-increasing gains in efficiency and performance. On the other hand, within the DoD there is often significant pressure to provide the troops with the best capability imagined in the first delivery increment. The irony is that a significant period of time passes during which nothing new is fielded.

The current DoD acquisition system also lacks the agility that is inherent in the private sector. Once texting became popular, for example, developers began to manufacture phones with full keyboards. They were able to do this in relatively short order because private industry is, by its very nature, acutely responsive to customer demand, creative in its solutions, and driven to maximize efficiency. The DoD, on the other hand, plays by a different set of rules: there is no profit motivation, inefficiency is permitted, and the customer base (i.e., the user community) is small in comparison.

Since nearly everything that the U.S. military needs in terms of IT is available in the private market, the DoD needs to leverage the best technologies from the private sector,

adapt them to their specifications, and deliver them quickly. The DoD's legacy acquisition approach was designed to facilitate the acquisition of DoD-unique systems. With regard to IT, however, this process is anachronistic and incapable of keeping pace with the rapid evolution of IT.

5. Security

Growing concerns over cybersecurity have added a new dimension to IT acquisition. The current system lacks robust, standardized security measures. Lone hackers and nation-states alike have made attempts to infiltrate U.S. government systems in order to extract classified information. In 2008, a Russian computer worm referred to as agent.btz infected the DoD's Secret Internet Protocol Router Network (SIPRNet) in what is largely considered the most serious breach of the DoD's classified computer systems to date (Nakashima, 2011). SIPRNet is not connected to the Internet, yet it is nonetheless vulnerable to worms and viruses. In the case of agent.btz, the worm was likely transmitted by a soldier whose infected thumb drive was inserted into a laptop connected to SIPRNet (Strategy Page, 2011). The DoD has yet to remove all traces of the worm from its network.

The threat is growing. Cyber attacks targeting government agencies' systems and websites increased by 40% in 2010. According to U.S. Cyber Command Chief General Keith Alexander, hackers probe the DoD's systems over six million times per day (Nakashima, 2011). And these "hacker groups" often include small groups of computer-savvy American teenagers, criminals, foreign terrorists, and, at times, even nation-states (foreign states have begun to invest in cyber weapons). Recently, a hacker group known as LulzSec attacked and disabled private websites and the CIA and Senate public web pages and has divulged information taken from law enforcement business systems. Their strategic purpose, if any, remains unclear. To counter cyber threats, the DoD must reduce its systems' vulnerabilities through more frequent upgrades. Secondly, it is essential that the DoD engage in an enterprise-wide expansion of its security standards and protocols

(Gallagher, 2010). Needless to say, the IT acquisition process must facilitate both of these initiatives.

III. Major Reports on IT Acquisition

Multiple independent studies of the government's IT acquisition process have been undertaken in the last few years in an effort to identify ways to improve the process's overall effectiveness, and although some have focused directly on the DoD's IT acquisition, others have sought to address the more general, government-wide challenges. We conducted a meta-analysis of these challenges and identified common threads with regard to process deficiencies and recommendations. Accordingly, our proposed acquisition process recognizes and adapts these commonly identified elements, attempting to correct the acknowledged deficiencies. The reports that we reviewed were produced between 2009 and 2010. They are listed as follows.

- The 2010 National Research Council's *Achieving Effective Acquisition of Information Technology in the Department of Defense*

  This report assessed whether the DoD could adopt best practices from the commercial sector for IT acquisition, systems engineering, and T&E. The report considered only those IT systems that support the DoD information enterprise and excluded IT-based components that are embedded in weapons systems or DoD-specific hardware. The report recommended that a new acquisition process be adopted, one that is tailored to IT, and that this process incorporate commercial-sector best practices.

- The 2010 U.S. House Armed Services Committee (HASC) Panel's *Defense Acquisition Reform, Findings and Recommendations*

  This report focused on two specific deficiencies of the current acquisition process: financial management and management of the industrial base. With regard to financial management, the report noted that poor resource allocation stemmed from the lack of commitment to improved accountability on the part of senior leadership. The report recommended that the DoD improve the audit readiness of each of the military departments, providing sanctions and penalties if necessary. With regard to the industrial base, the report recommended that the DoD better analyze commercial price trends to ensure proper pricing. In addition, the report recommended that the DoD provide better

visibility to contract solicitations to ensure a level playing field, especially with regard to small businesses.

- The 2010 TechAmerica's *Government Technology Opportunity in the 21st Century: Improving the Acquisition of Major IT Systems for the Federal Government*

  This report asserted that stronger program oversight, better risk management, and greater agility are key to improving IT acquisition within the federal government. The report recommended that the government build a professional development program for IT program managers, use third-party independent risk reviews to assess IT projects, and promote more engagement between industry and government. The report asserted that agile development can only succeed when an incremental process is used and that incremental processes are, in turn, only successful in an interactive and collaborative environment.

- The 2010 Association for Enterprise Information's *Industry Perspectives on the Future of DoD IT Acquisition*

  This report offers "unsolicited views of a team of industrial and academic experts" on the implementation of a new acquisition process. The report recommends that the DoD "institute continuous, iterative, development, test, and certification processes that drive the commercial IT state-of-the-art commercial to deliver off-the-shelf building blocks" for the DoD's systems (p. ii).

- The 2010 IT Acquisition Advisory Council's *A Roadmap for Sustainable IT Acquisition Reform: Congressional Summary*

  This report summarizes the specific challenges that agencies face in executing existing IT policy and agency mission objectives. The report highlights the need for a more agile non-weapons system acquisition approach to IT. The report suggests that the new process embrace IT cloud infrastructure, which would provide the majority of applications as software services. In addition to adopting a new IT process, the report recommends that

the DoD implement supporting initiatives centered on transparency, culture change, leadership, oversight, and an improved acquisition workforce.

- The 2009 Government Accountability Office's *DoD Needs to Strengthen Management of its Statutorily Mandated Software and System Process Improvement Efforts*

  This report assessed the extent to which the DoD has implemented certain software and systems process improvement actions mandated in the National Defense Authorization Act for FY2003. The GAO concluded that weaknesses still exist with regard to system and software acquisition and the development process. The GAO also provided examples of cost, schedule, and performance shortfalls across a range of DoD software-intensive programs.

- The 2009 Defense Science Board's *Department of Defense Policies and Procedures for the Acquisition of Information Technology*

  This report undertook an extensive review of DoD policies and procedures for the acquisition of IT. The report examined acquisition and oversight policies and procedures, roles and responsibilities for acquisition officials department-wide, and reporting requirements and testing as they relate to IT acquisition. The report concluded that the DoD should adopt a unique acquisition process for IT and that such a process must be designed "to accommodate the rapid evolution of information technologies; their increasingly critical position in DOD warfare systems, warfare support systems, and business systems; and the ever evolving and often urgent IT needs of our war fighters" (p.10).

All of the reports concluded that the current acquisition process is ill-suited to the acquisition of IT and described the inability of the process to efficiently deliver IT systems on time and on budget. The reports cited numerous deficiencies with regard to the process, product development, workforce, and management. These deficiencies are summarized as follows.

- Process Deficiencies

One major point of failure is that the Defense Acquisition System process tends to stall at milestone decision points. When a system reaches these milestones, programs must gain approval from many different functional organizations. It can take up to 90 days for a milestone decision to be reached (DSB, 2009). When one considers that commercial IT is on an 18-month development cycle, these delays are not tolerable. When a product that has been delayed is finally released, it is often the case that the requirements, technology, and standards have changed. In addition to the milestone decisions, excessive program documentation requirements create additional delays and shifts, which distance the existing process from commercial best practices.

Applying the Defense Acquisition System approach to the acquisition of defense business systems generally does more harm than good, since the threshold of risk management that the Defense Acquisition System requires is higher than the risk associated with the mature technology used to produce defense business systems. Because the Defense Acquisition System is designed to reduce the risk associated with multibillion-dollar, complex weapons programs, repetitive and detailed reporting requirements are designed to provide improved visibility so that program personnel can identify problems early on. With their longer duration—from JCIDS initiation to full deployment—changes are much more likely to occur (HASC, 2010). For this reason, repetition of reporting requirements may be less of an issue and may merit the additional time and resources. However, because defense business systems can be developed with less inherent risk—and in one-tenth the time—extensive and repetitive documentation is problematic.

Finally, continuous T&E must occur throughout IT development cycles. Because defense business systems are highly dependent on stakeholder feedback, continuous T&E ensures that this feedback is integrated into the product as efficiently as possible (in the form of new features, more intuitive design, and so forth). Continuous T&E obviates the need for the intensive redesign that often occurs following large blocks of untested development. Under the Defense Acquisition System, T&E supports a specific phase of development, which, for

physical systems and platforms, may be the only way to effectively evaluate a program. However, for IT systems, the lack of continuous T&E causes delays and cost overruns while limiting the potential effectiveness of the product.

- Development Deficiencies

The DoD has a clear need for integrated enterprise-wide business solutions. COTS products can help meet this need. While it is true that COTS solutions are sometimes inappropriate within the context of major weapons acquisitions, this is not the case with regard to defense business systems. The DoD is, after all, an organization that requires much of the same infrastructure as any other large business enterprise.

Although COTS-based sourcing is recommended in DoDD 5000.1 and DoDI 5000.2, in practice, it continues to face significant resistance. In part, this stems from an unwillingness to adapt certain business processes (National Research Council, 2010). For instance, there is often significant pressure to provide the troops with the best capability. This translates to the formation of specific requirements, some of which are Service-unique and technologically challenging. Additionally, it is thought that in adopting COTS solutions, the Service branches necessarily relinquish control over programmatic elements. But even when enterprise-wide systems are not COTS-based, control and requirements issues arise. For example, in the case of the DIMHRS program, referenced in the previous section, the Navy resisted system implementation because DIMHRS lacked requirements that the Navy believed were essential.

The procedural impact associated with the capabilities development document (CDD) and contract also creates an aversion to COTS sourcing. A CDD is “a document that captures the information necessary to develop a proposed program, normally using an evolutionary acquisition strategy. The CDD outlines an affordable increment of militarily useful, logistically supportable, and technically mature capability” (Defense Acquisition University [DAU], 2011). In the Defense Acquisition System, the CDD is used to support and inform the Milestone B decision, which authorizes entry into the Engineering and Manufacturing Development (EMD) phase. It includes requirements and expectations for the program that

must be completed at each phase of the acquisition program, up to and including deployment. Since the system relies on a single CDD, programs aim to achieve a 100% solution upon the initial capability release (Armour, 2002). The program's "big bang" requirements slow the process by creating more documentation and longer development phases. Luckily, for IT programs, post-release upgrades are much easier to integrate, as demonstrated by the agile, incremental approach to software production used within the commercial sector, an approach that facilitates the addition of marginal improvements over time (Lapham et al., 2010). Thus, the "80% solution" that COTS products often provide is entirely appropriate with regard to IT.

- Management Deficiencies

Developing and implementing IT systems requires technical knowledge that is both specific and extensive. Because the DoD does not have a separate IT acquisition process, even program managers who have proven highly successful at managing weapons systems acquisitions may not be adequately prepared to take on IT systems management. Currently, the DoD does not require managers to have IT-specific knowledge and experience to manage IT programs, nor does there exist training courses designed to enhance technical skills (DSB, 2009). As a result, the DoD relies heavily on service contracts with the private sector to manage its IT acquisitions.

In addition to program management, strategic management has also been highlighted as an area of concern. Strategic management is provided through regulations from the Federal Acquisition Regulation (FAR), Defense Federal Acquisition Regulation Supplement (DFARS), and other legislation. These regulations have proven crucial to controlling cost overruns in the past and to providing Congress with the ability to maintain its oversight role over the DoD. With regard to IT acquisition, one of the most critical regulations is Section 804 of the 2010 National Defense Authorization Act, which mandates the development and implementation of a new IT acquisition process. While this act is certainly a step in the right direction, it is true that congressional oversight has, on occasion, created ambiguities in the DoD's acquisition strategy. For instance, the Goldwater-Nichols Act, the Clinger Cohen Act,

and the 2005, 2007, and 2009 NDAAs lacked clarity with regard to specific features of their implementation.[7] Rather than promoting innovation and flexible responses to acquisition problems, the ambiguities led to the creation of more structure, which, in turn, increased the amount of documentation. Although these congressional acts may have reduced systemic risk, they also prompted cost increases and programmatic delays.

There were also commonalities with regard to the recommendations contained in the reports. Based on our analysis, we have identified what we believe to be the most important recommendations.

- Develop a new, separate IT acquisition process.
- Take advantage of the agility afforded by incremental development approaches, economies of software reuse, and ubiquity of web-based commercial products.
- Embrace established standards and an open systems approach.
- Use standard systems that support uniform security requirements, rather than develop independent solutions for each program or increment.
- Break typically large programs into small, incremental developments that are quickly delivered within the same IT generation.
- Provide continuous or short cycle oversight rather than oversight based on long-term milestones.
- Generally, require less documentation.
- Use lower level documents to define capabilities at the increment level.

[7] These federal laws continue to complicate the acquisition of the DoD's IT systems (i.e., Goldwater-Nichols, Clinger-Cohen, and the NDAA FY2008). They cause overlapping responsibilities between the Under Secretary of Defense (AT&L), the Department's CIO, and the Deputy Chief Management Officer.

- Use business case analyses more broadly and as a basis for analysis and justification for increment approval.
- Incorporate early and continuous user involvement in the process.
- Use iterative prototyping to reduce risks and shorten the overall process.
- Blend the current multiple program test events into a single process rather than individual tests that start and stop independently.
- Ensure flexibility in contracts to allow for required changes as they occur.
- Make funding as flexible as possible for increments within programs.
- Provide stable funding.
- Set high-level, “big-R” requirements at the outset of a program.
- Develop detailed requirements throughout the acquisition process (program management).
- Develop and retain a cadre of IT domain experts to support oversight and decision-making (DoD acquisition workforce).

We have incorporated these recommendations into a new acquisition process: *IT 360*.

IV. *IT 360*

The *IT 360* process is a revolutionary approach to IT acquisitions that results in rapid acquisition and provides continuous iterative and incremental delivery of useful, affordable, and architecturally compliant capabilities with adequate oversight, reporting, and documentation. *IT 360* increases end user functionality while encouraging competition throughout the process—from program inception to retirement. The proposed use of COTS, standards, and existing capabilities to the maximum extent practical reduces development and unnecessary engineering, testing, and support costs. These programs, however, will require active engagement with functional management and users throughout the development process as well as flexibility throughout development, testing, and contracting. Ultimately, the process will be able to produce effective systems quickly, at less cost and with less risk.

The *IT 360* process is specifically tailored to the acquisition of defense business systems. Embedded within *IT 360* are a series of initiatives, which, we believe, will allow the DoD to enhance the speed and efficiency with which it acquires its defense business systems. These initiatives are described in detail in the following subsections.

1. Spiral Development

The *IT 360* process is based on the concept of spiral development. Since 1988, spiral development has served as the prevailing commercial model for developing software. Spiral development is a cyclical approach to incrementally growing a system's capabilities while decreasing risk. Unlike sequential development processes whereby a product's features are prescribed early on, spiral development is agile and responsive, incorporating innovations that arise during development. Because the base architecture does not change, the spiral development process adds functionality to a system's existing capabilities at a quick, standardized pace (Lapham, Williams, Hammons, Burton, & Schenker, 2010). This allows development teams to leverage what they have learned from each of the previous iterations and adjust specifications and capabilities as needed to increase program and system efficiency.

2. Smaller, Quicker to Deliver, Useful Sets of Capabilities

Large programs are broken into smaller, agile increments that are responsive to innovation and new technology, allowing for the rapid development of new capabilities. These rapid incremental developments allow program managers to quickly identify and mitigate program risk as it arises. As a result, managers are able to communicate program status to stakeholders quickly yet comprehensively. Smaller increments carry less risk, thus permitting the delegation of decision-making authority, which enables more timely decisions by people who are directly involved in the program. These officials are in the best position to accelerate, redirect, or cancel an increment's release. Each increment can then be integrated into a system of systems environment, which is seldom the case under the traditional acquisition process. Accordingly, incremental delivery requires less overhead.

3. Rapid Delivery

Time-to-delivery is a key objective (perhaps even a key performance parameter) for every IT program. *IT 360* programs will rigorously employ a scheduling concept whereby traditional milestones and key decision points are established early on, and these are scheduled in much shorter periods. For example, the time allocated to complete a business case and program implementation plan (leading to a build/procurement decision event) is much shorter (approximately 30 days) under *IT 360*. Similarly, capability releases occur on an accelerated schedule (i.e., initial increment capability delivery occurs 360 days after program initiation). When coupled with the smaller increments, the release of subsequent iterations will vary depending on the nature of the program but will occur on a schedule established by program managers.

4. Greater Use of COTS Products

Incorporating the greater use of COTS products into IT programs is essential if the DoD is to shorten its acquisition time lines and reduce costs. Like the DoD, large corporations rely on business systems for a host of different reasons, including payroll, accounting, supply chain management, and the delivery of goods and services to customers. Today, most business

software is developed in the commercial sector. Given the similar needs of private enterprise and the DoD, it stands to reason that the DoD should look to the commercial sector to procure its business systems or, at the very least, core system components.

COTS products are advantageous because the development, T&E, and security measures have already been completed and funded by the private sector. Furthermore, because COTS are available for purchase within the private sector, the market has set the price, which ensures that the DoD is not overpaying. As mentioned previously, even if a COTS product does not fulfill all of the necessary requirements, the DoD can elect to modify the product or integrate it into another system. Moreover, since COTS products incorporate mature, proven technologies, the risk to the DoD is minimized. Currently, COTS products are underutilized by the DoD, primarily because they fail to meet all of the "small-r" requirements, which, by definition, are often not mission critical. Frequently, the marginal benefit of these small-r requirements can be offset by other features that are built into the COTS product over time.

Use of proven capabilities that are pre-tested and pre-certified will accelerate deliveries of capabilities and shorten time lines while reducing costs and delivering useful, architecturally compliant capabilities within the established time frame.

5. Aggressive Use of Prototypes and Demonstrations

DoD acquisition programs often rely on pilot programs and demonstrations of capabilities as a means of reducing risk. Requiring a product—be it a C-5 aircraft or a payroll software program—to operate in a real-world environment, as opposed to the theoretical one in which it was conceived, allows program personnel to identify problems prior to the product's fielding. Prototypes and demonstrations incorporate, at minimum, a basic level of development that can be later incorporated into the full program upon approval. The *IT 360* process will encourage the delivery of prototypes and demonstrations by the vendors, along with their proposals. These will be used during source selection, reducing technical risk and enabling the selection of developers and integrators with a demonstrated ability to implement the required system. Finally, in some circumstances, they will serve as the initial increment upon which increased capabilities are evolved over time.

6. Continuous and Integrated Testing

With weapons system programs, serial T&E prior to production is essential to the development of weapons systems. IT development, however, requires a continuous cycle of testing during development—blending software qualification testing (SQT), DTE, OTE, and interoperability. Moreover, by including representative operational data sets and simulation tools, program managers can help ensure the release of refined, useful capabilities using stressful operational environments. As a result, these tests occur in a near-operational environment prior to fielding, which helps to ensure interoperability, compliance, and compatibility with DoD architectures, standards, and operating environments. Because testing is continuous, security vulnerabilities, hyper-specified and unnecessary features, and other potential problems can be identified quickly. By permitting operational experience to inform future product requirements, *IT 360* ensures that systems are optimally suited to the needs of their users.

7. Decentralized Execution

More frequent product reviews serve to enhance the relationship between the program manager and senior-level authorities as well as to facilitate more timely decision support from acquisition staffs and the oversight community. Because each increment has defined capabilities and is released according to a set schedule, there is less financial risk. Accordingly, there is less need for burdensome oversight and the associated documentation requirements that are built into the current acquisition process.

8. Inclusion of End Users

Including users and other stakeholders throughout the process allows program personnel to better understand mission needs. Similarly, the user community is better able to understand product capabilities when they attend regular meetings with program officials and are part of the decision-making process. Additionally, encouraging user engagement throughout product testing is crucial in that user feedback helps to ensure that simulations occur in realistic operating environments. Providing users with early prototypes enables them to adopt existing processes to

new capabilities while at the same time allowing program personnel to more efficiently incorporate users' emergent behaviors.

9. Enhanced Competition

Competition is a driving force in the U.S. economy and a vital component of efficiency and improved market performance in both the public and private sectors. It provides incentives to produce better products faster, at lower costs, and with better quality: this has been proven repeatedly. *IT 360*, with its smaller increments and shorter cycles, enables competition at the launch of each new iteration.

10. Cybersecurity

While this report does not address cybersecurity in any detail, we recognize that maintaining cybersecurity is of the utmost importance. This critical issue must be considered throughout the IT acquisition cycle, to include the post-implementation operational procedures. The use of data standards, open architectures, COTS, and modular products will enable the implementation of up-to-date technology, also facilitating strengthened system security.

The *IT 360* Process

IT 360 is both an evolutionary and an incremental approach to IT acquisition. Indeed, the initial *IT 360* product iteration may not possess all of the desired capabilities. However, the process is intended to be continuous and seamless, completing each 360-degree cycle in approximately 360 days. The objective is to more closely match the development cycle of commercial IT systems. Therefore, once the base architecture of the required IT system is established, the *IT 360* process adds functionality to the system's existing capabilities at a quick, standardized pace. Development teams leverage what they have learned from each of the previous iterations and adjust specifications and capabilities as needed to increase program and system efficiency and functionality. In short, *IT 360* allows for the gradual refinement and improvement of a system over multiple iterations. This process is depicted in Figure 3.

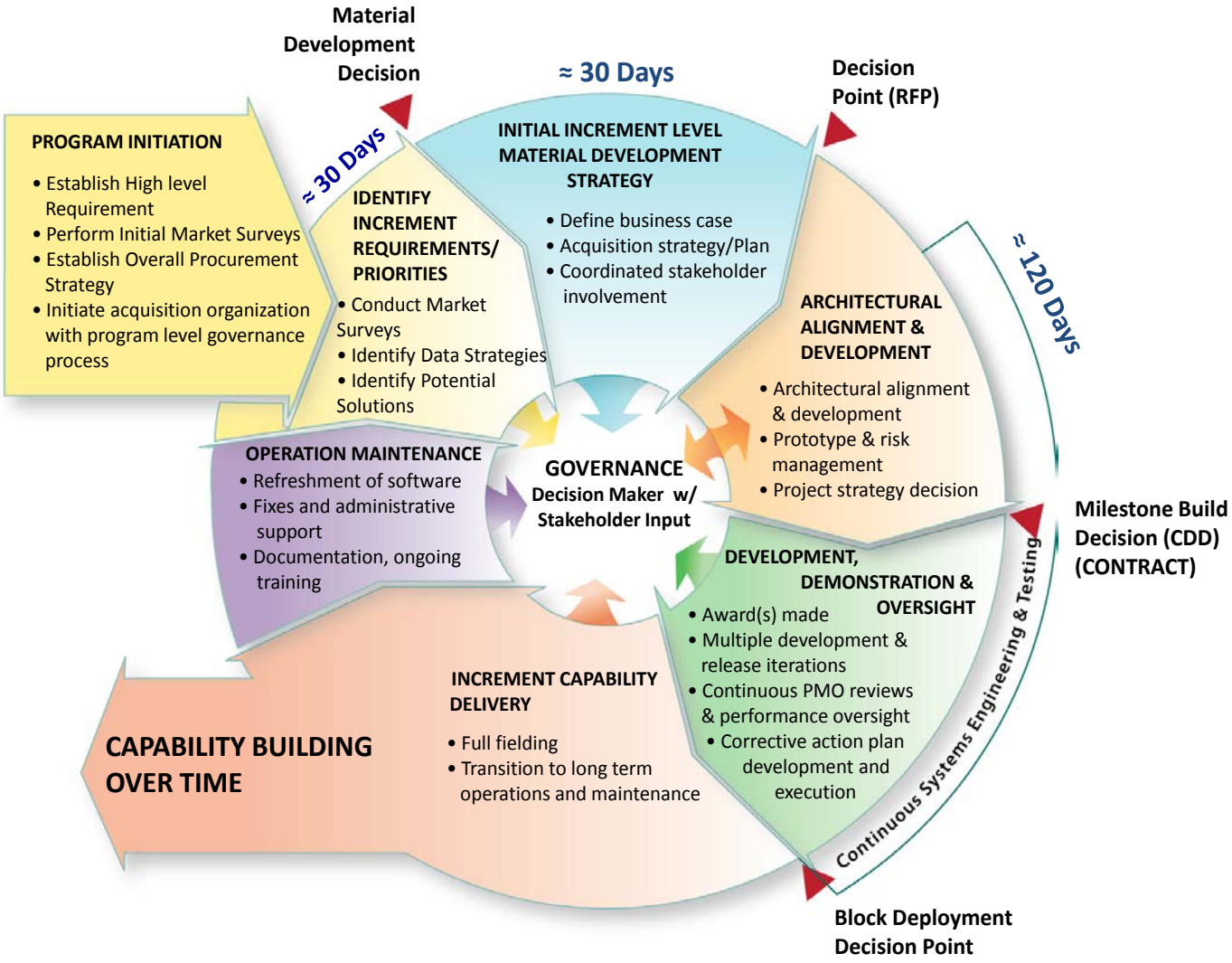

Figure 3. The *IT 360* Process

Note. Initial increment capability delivery occurs 360 days after program initiation, at which point the process will have completed one 360-degree cycle.

The seven phases of the *IT 360* process and their objectives and durations are summarized as follows.

Phase 1: Program Initiation

The *IT 360* process begins with a Program Initiation phase. The initiation phase lays the foundation for program acquisition in four distinct ways. First, initial market surveys are conducted in order to generate potential solutions and establish a successful acquisition strategy. Using this strategy, the high-level requirements for the program are determined. These high-level requirements—sometimes referred to as "big-R" requirements—specify general system capabilities. Less emphasis is placed on minor requirements (the over-specification of which often leads to cost overruns and delays); rather, minor requirements are deferred to future increments. Next, both the high-level requirements and the market surveys are used to establish the overall procurement strategy, which will inform future phases over multiple iterations. Support contractors may be relied upon to develop the system's architecture or to provide systems engineering. Once the strategy is established, program- and portfolio-level governance are then created and initiated.

Phase 2: Identification of Increment Requirements and Priorities (30 days)

After a program has been initiated, it enters the Identification of Increment Requirements and Priorities phase. During this phase, all potential solutions are considered, including COTS and other open-source solutions. Solutions are evaluated based, in large part, on how well they enable data transfer. In the past, the ease with which existing data could be transferred to new systems was overlooked, requiring thousands of hours of labor of manual input. With a total duration of approximately 30 days, the secondary goal of this phase is to ensure that capabilities are assigned to appropriate increments. By continuing the market surveys begun during the Program Initiation phase, program personnel work to ensure that the initial requirements meet as many user demands as possible, without front-loading onto early increments the more difficult, though perhaps nonessential, requirements. This is an important distinction over the Defense

Acquisition System process, which has a tendency to "waterfall" requirements, leading to increased rigidity throughout the process. This phase concludes with a material development decision (MDD).

Phase 3: Initial Increment Level Material Development Strategy (30 Days)

After a program has been approved through the MDD milestone, the Initial Increment Level Material Development Strategy phase begins. During this phase, a procurement strategy that is both product-specific and increment-specific is devised. While much of this strategy was developed during the previous phase, it is during Phase 3 that program personnel delineate a highly-structured, comprehensive business case (i.e., program justification) and a fully developed acquisition plan and develop a mechanism that ensures coordination of stakeholder involvement. With an approximate duration of 30 days, this phase finalizes development and planning for the initial increment. The Initial Increment Level Material Development Strategy phase is completed upon the approval of a request for proposals (RFP) by the Program Governance Board (PGB).

Phase 4: Architectural Alignment and Development (120 Days)

After the release of an RFP to private-sector contractors, the Architectural Alignment and Development phase begins. This phase, which marks the beginning of system development, has a duration of approximately 120 days. The PMO may need to contract for the necessary technical expertise to assist in writing statements of work and/or provide objective analyses of government or contractor progress toward meeting system development goals. For ease of upgrades, standards-based open architecture is strongly encouraged; this will preclude a specification that is based on a proprietary product and avoid restrictive intellectual property rights issues and vendor lock-in.

Once the architecture is determined (i.e., the strategic, programmatic, and incremental requirements set forth in the proposal are approved), a risk assessment is conducted via prototyping and other methods. Appropriate risk reduction strategies are then implemented. Once it is determined that the architecture carries sufficiently low risk, Phase 4 concludes, which prompts the issuance of the CDD. The CDD clearly details why the system is needed; how it

will be used; where the system will be located; who will need it; when it will be available; what the system is intended to do; how the system will be supported; and how much it will cost. Contracts are written to reflect the information contained in the CDD.

Phase 5: Development, Demonstration, and Oversight (180 Days)

The issuance of a CDD marks the beginning of the Development, Demonstration, and Oversight phase, as well as the contract award. With an approximate duration of 180 days, it the longest phase of the *IT 360* process but also the most crucial. At this milestone, the decision authority approves the acquisition strategy, enterprise contracting/buying strategy (lease/buy, buy as a service), increment level detailed requirements, and market and spend analysis, acquisition program baseline, program implementation plan, test plan, and documentation. During this phase, the program manager will manage the development and demonstration of the proposed IT solution for a release of capabilities within specified cost, schedule, and performance parameters. Further, procurement strategy should call for the purchase of only the software license quantities needed to complete integration, testing, and demonstration. The remaining license quantities needed for full system deployment are deferred until after successful T&E and demonstrations.

Additionally, during this phase, multiple iterations of the system may be developed and tested (T&E is integrated into each iteration). Upon the release of each iteration, stakeholder input, oversight, and if appropriate, corrective action are combined to guide development of the next iteration. When successful, the program manager can rapidly deploy the capability or continue to demonstrate the capability in a live operational environment, depending on the nature of the program.

Phase 6: Increment Capability Delivery

Assuming that the system fulfills the strategic, programmatic, and incremental requirements, the PGB will authorize its entry into the Increment Capability Delivery phase. This phase has two main functions: full fielding and the transition to long-term operations and maintenance (O&M). Depending on the circumstances, fielding might include the product's integration into other systems or services or the transfer of data from old systems to the new system. The second

function is the transition of the product to long-term O&M. This entails the creation or augmentation of a support structure specifically tailored to the capabilities of the newest product iteration.

Phase 7: Operations and Maintenance

The Operations and Maintenance phase oversees the creation or augmentation of a support structure specifically tailored to the capabilities of the released product. This entails complementary documentation and ongoing training in support of the recent release, refreshment of software, bug fixes, and administrative support. Because future increments have new capabilities, the O&M phase is critical in that it ensures that previously released increments are able to interoperate seamlessly and securely with earlier versions.

Entrance into this phase depends heavily on the user's satisfaction with the solution and willingness to use the IT capability in the operational environment. The support plan is executed to meet the operational needs of the IT system in the most cost-effective manner. This plan will identify strategies to respond to discrepancies, failure reports, and hardware and software updates and upgrades.

Supporting Initiatives

To maximize the benefits of the *IT 360* acquisition process, we have identified four supporting initiatives: (1) documentation streamlining, (2) flexible contracts, (3) tailored program financial management, and (4) forward-looking standards and technology neutrality. These initiatives are described in the following subsections.

Documentation Streamlining

Program documentation serves two purposes. First, it helps to ensure that program requirements are understood and executed properly by the contractor, which reduces risk to the DoD. Second, documentation is used to provide program personnel with program status and updates. Under the current Defense Acquisition System process, the level of documentation varies and depends, in large part, on the program's ACAT designation (10 U.S.C. 2445(a)). Requiring extensive and

excessive documentation results in longer acquisition time frames and higher costs and increases the likelihood of miscommunication between the DoD and the contractor. These requirements unnecessarily complicate IT acquisition programs. Consequently, a fundamental tenet of any IT acquisition process must be to require "just enough" documentation. Documentation should be tailored to mitigate risk while reducing reporting burdens. Further, since similar programs are likely to face the same risks, programs should be grouped into categories based on their shared similarities. Standardized, category-specific documents could then be created and used by programs within each group. The governance bodies must ensure that documentation requirements are consistent with this principle of "just enough" and that required reviews are completed quickly. Indeed, many of the reports listed in Section II recommended that such an approach be used not only within the DoD but also across the federal government (Acquisition Solutions, Inc., 2009).

Moreover, programs should promote the reuse of standardized documents. Currently, documents are completed at multiple points throughout the acquisition process, although these documents often reflect no new data (Drezner et al., 2006). Each document, its submission, and its subsequent evaluation requires time and money to complete, thereby eroding the efficiency of the acquisition process. Indeed, the government and its contractors often hire document specialists to facilitate this process, which increases program overhead and, thus, the cost to government. By authorizing the reuse of standardized forms throughout the process in order to eliminate redundancies, efficiency could be increased.

Further, establishing document page limitations could also serve to further reduce the burden for both reporting and reviewing entities and allow for quicker decisions. In addition, because the commercial sector is driven to improve efficiency in order to maximize profits, it strikes the right balance between documentation burden and risk mitigation. Accordingly, the DoD should consider adopting a documentation strategy that leverages the proven practices of the commercial sector by adhering to similar standards.

Finally, various technologies can be used to replace some of the required documentation. Online collaboration and status dashboard software are two such technologies. Online collaboration

software allows multiple entities to simultaneously share data and multimedia on a shared digital workspace anytime, anywhere. In addition to online collaboration, electronic status dashboards should be used, either independently or in conjunction with online collaboration. Often, information reported via status dashboards is coded to reflect its importance; an imminent problem might generate greater visibility to attract the attention of certain stakeholders, allowing issues to be identified and resolved more quickly. Currently, program personnel and decision-makers are frequently alerted to problems only after they occur, because the needed information is embedded in a lengthy report that is released only at a certain point within the acquisition process. Status dashboards allow personnel to home in on the information that is most critical without having to sort through superfluous documentation.

Flexible Contracts

Currently, most contracts contain rigid requirements. Yet despite this rigidity—or perhaps because of it—current contract structures frequently fail to incentivize innovation; rather, contractors appear more or less content to meet the minimum requirements. More agile contract vehicles must be pursued to encourage greater private- and public-sector collaboration. Indeed, the commercial sector has begun to rely on innovative, flexible contracting and has been successful in reducing risk, using new contracting vehicles in combination with spiral development. Since the addition, removal, and alteration of requirements is expected as a program progresses in order to benefit from stakeholder feedback, contracts should be flexible enough to reflect this ongoing requirements definition.

Further, costs can be reduced in both the short and long terms by frequently interjecting competition at various points throughout the process. Moreover, since contractors bid only on work for one iteration, there is a strong incentive to provide the best value—especially when relevant prior experience and results is considered in the award. To maximize flexibility, portfolio-level contracting should be used because it allows managers to readily add or divert funding to a host of programs as needed.

Tailored Program Financial Management

It is difficult to fund emerging technologies or adapt standards between budgetary cycles; although funding can be appropriated from the next fiscal year's budget, doing so usually causes delays, which, as explained previously, decrease the effectiveness of the *IT 360* process and, thus, the utility of the defense business system in question. Unfortunately, tailoring current financial management practices may prove difficult. 31 U.S.C. 1301 dictates that "appropriations shall be applied only to the objects for which the appropriations were made except as otherwise provided by law." We advocate for a more flexible funding mechanism (e.g., multiyear portfolio accounts). The introduction of such mechanisms may necessitate changes to current law, an issue we explore in more detail in Part V of this report.

Forward-Looking Standards and Technology Neutrality

The use of forward-looking standards (i.e., those that facilitate a product's technical evolution, rather than constrain it) will assist developers in meeting both the big-R requirements and the small-r requirements. To the maximum extent practical, standards should be based on those that have already been developed for the commercial sector.

Relying on commercial standards helps to ensure an IT product's relevance and longevity. In instances where it has developed its own unique standards, the DoD has experienced both failure and success. For instance, in 1977, the DoD began development of the programming language Ada, the use of which was later mandated for practically all DoD software. The DoD adopted a series of policies to encourage the endorsement of Ada as the universal commercial standard, to be used in designing all embedded systems. It went as far as to mandate its use in all DoD software applications. However, despite these efforts, Ada was never widely adopted, and because the commercial market dwarfed the military market, it eventually fell out of use, even within the DoD (Chapin, 2004).

In 1997, the DoD began development of the Joint Tactical Radio System (JTRS). An open systems framework known as the Software Communications Architecture (SCA), developed by the program, was key to the system's interoperability. Even though the JTRS program has had

some major challenges, the SCA has been a real success and is the de facto standard for all software-defined radios, to include those developed commercially. Despite this success, the development of new standards should only be pursued when acceptable standards do not exist within the commercial sector. Commercial standards generally support the design of modular products. As mentioned previously, the DoD must seek to maximize the modularity (i.e., the degree to which the rules of the system architecture enable or prohibit the mixing and matching of components) of its IT products. Indeed, commercial standards can be leveraged not only to smooth the transition between current IT and future IT systems, but also to augment the capacity of the DoD's IT infrastructure by facilitating the development of a vast network of IT products and systems that collectively offer greater functionality than the sum of the products within the network.

In addition to the use of standards, adopting a technology-neutral approach will reduce programmatic risk by facilitating data reconciliation and migration. In July 1997, President Clinton and Vice President Gore released a report entitled *Framework for Global Electronic Commerce*, which stated, "rules should be technology neutral (i.e., the rules should neither require nor assume a particular technology) and forward looking (i.e., the rules should not hinder the use or development of technologies in the future)" (p.1). An example of an effective technology-neutral approach is a service-oriented architecture (SOA). SOA is an IT approach that relies on the separation of architectural layers to ensure interoperability and compatibility when designing software. This approach allows developers to package functionality as a suite of interoperable services. With this approach, these services are generally well-defined functionalities that are built as software components that can be reused for different purposes.

IT 360 Governance Structure

The *IT 360* governance structure was designed to promote stakeholder integration, speed, and ease of access. Overlapping governance is a key structural attribute of the *IT 360* process that enhances the success of IT acquisitions. Traditionally, the majority of oversight takes place prior to program milestones and at key decision points within a specific program or portfolio of programs.. While oversight is present at these points, it is also integrated into each of the phases.

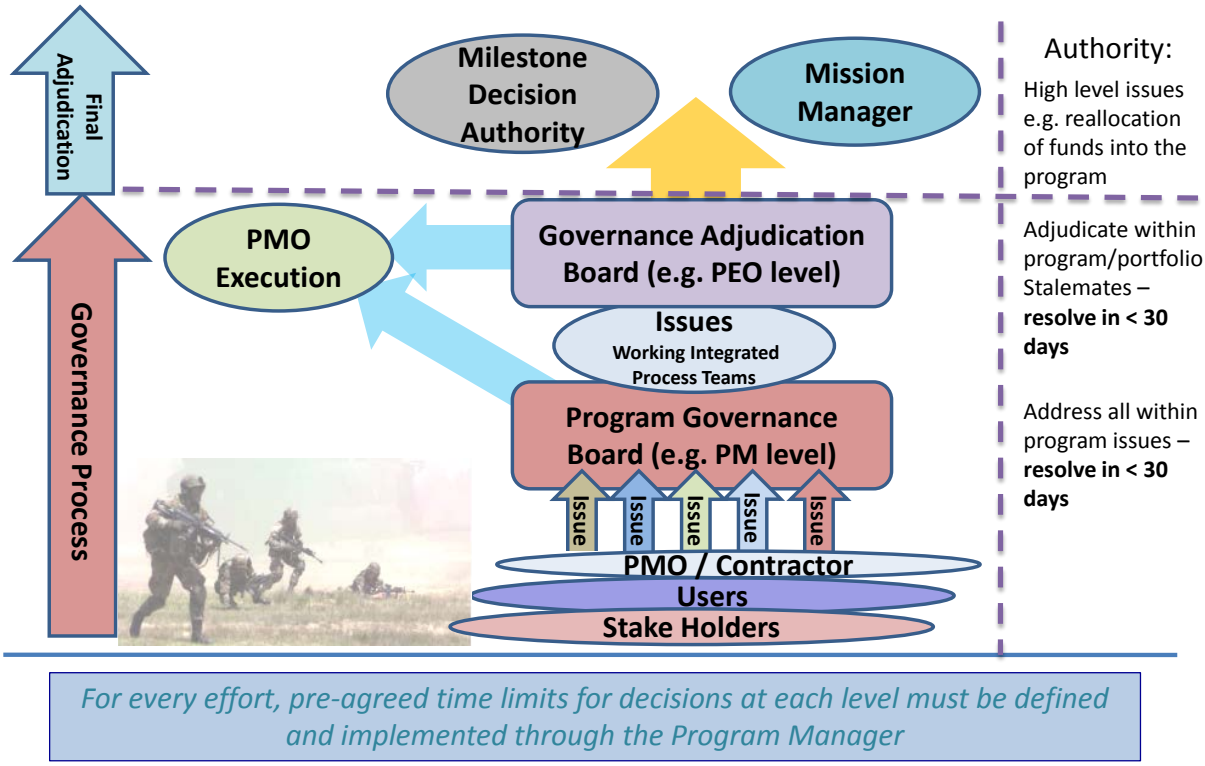

Figure 4. *IT 360* Governance Structure

One of the primary goals of the multi-tiered *IT 360* governance structure is maximizing internal adjudication (see Figure 4). When a problem or issue is brought forward by the program office/contractor, user, or other stakeholder, it is immediately brought to the attention of the PGB, which is composed of officials at the program management level. In conjunction with stakeholders, the program governance board identifies a solution and provides a corrective action, which is then executed by the PMO in the event that the issue cannot be resolved or if consensus is not obtained, the problem is elevated to an issue-based working group. These working groups are integrated process teams consisting of a program office representative, contractor personnel, and members of the user and stakeholder communities. These entities are highly invested and, collectively, highly knowledgeable about all program areas. After the team formulates solutions to the problem in question, these solutions are forwarded to the Governance Adjudication Board (GAB). This board is at the level of the project executive officer (PEO); as such, it is able to grant greater authority to the decision. As with the PGB, if and when

consensus is reached, the solution is forwarded to the PMO for execution. If, however, another stalemate occurs, final adjudication is provided by an upper-tier authority, usually the mission manager.

Requirements, for example, will mature over time, and governance mechanisms must be structurally and institutionally prepared to deal with these anticipated requirement changes. The PGB would track, adjudicate, and resolve changes and make assessments of changes for their potential impact.

The tiered structure depicted in Figure 4 was designed to minimize delays in decision-making. This is accomplished by streamlining the milestone decision process, incorporating more governance between milestone decisions, and making more efficient use of documentation. The lower tier consists of PGB personnel who work within the program or portfolio and oversee all activities. While the upper tier has responsibility for multiple programs, along with the authority to adjudicate all decisions within the program, it is primarily concerned with high-level issues and the resolution of stalemates. High-level issues could include, for example, the reallocation of funds among programs or the strategic realignment of programs. Intra-program issues, such as the reallocation of funds within a program or portfolio, on the other hand, would be carried out by PGB-level personnel. This represents a significant change in responsibility; generally, a program's internal funding allocation is the responsibility of the PEO (lower tier). The *IT 360* governance structure has the potential to reduce delays and enhance programmatic success by granting decision-making authority to those most familiar with the inner workings of the program, which, in turn, reduces the overall administrative and documentation burden. Furthermore, *IT 360* governance requires that program managers define and implement pre-agreed time limits for all decisions. One of *IT 360*'s stated objectives is to resolve issues within 30 days or fewer or elevate the problem to the GAB, which, in turn, must resolve the problem in 30 days or fewer or elevate the decision.

V. Challenges and Barriers

The *IT 360* process has the potential to transform the DoD's approach to IT acquisition. However, for this transformation to take place, a number of specific challenges and barriers must be overcome.

Challenges

These challenges revolve around the following longstanding issues: contracting practices, funding, industry cooperation, competition, requirements, cybersecurity, and workforce.

Contracting Practices

The accelerating pace of change of information technology, particularly in the commercial sector, requires greater contract flexibility in order for the DoD's business systems to remain current. Contracts must be structured to reflect incremental developments and decisions as well as the evolving requirements definition. For example, when using a rapid-cycle, spiral approach, program managers will need flexibility to defer requirements to the next increment on their own authority. DoD contracting practices, however, generally do not provide programs with this level of flexibility. Even where the DoD attempts to adopt commercial approaches and practices, government contracting differs significantly from commercial practices because of regulatory and legislative factors. These factors include fiscal constraints, requirements for transparency, and the required audit and oversight. As a result, attaining the desired contract flexibility is a challenge.

Furthermore, flexible contract frameworks for common products and services should be contracted at the portfolio level (i.e., across programs). Given the degree to which IT programs, their objectives, and their requirements are interrelated, portfolio-level, flexible contracts increase efficiency while minimizing the costs associated with contract writing and oversight. Whenever possible, programs should use proven commercial practices, including performance-based contracts. DoD programs should also take into account past performance and experience with similar efforts. In order to incentivize the greatest level of innovation, lowest price,

technically acceptable (LPTA) criteria should be avoided as the source selection criterion, except for the most routine of services.

Funding

For reasons similar to those mentioned previously, flexible funding is crucial to the success of the *IT 360* process, and its provision lays the groundwork for programmatic success. Currently, with the lengthy budget process, it can take as long as three years to define a requirement well enough to request funding. This lengthy process creates a perverse incentive to buy IT capabilities in large, long-term lots—which is exactly the wrong approach. Development teams, however, need to be able to take advantage of opportunities as they arise or to avoid technical difficulties as necessary. As requirements evolve between spirals, programs need greater latitude to realign funds within the scope of the total program, if necessary. Consequently, to support a fast-paced, agile IT acquisition process will require a more agile budgeting process, particularly when the requirements for subsequent increments of capability are not yet sufficiently defined.

Program executives must be able to allocate and divert funding based on a particular program's progress in meeting its objectives. An alternative approach is for the DoD to adopt a "level-of-effort" funding model at the portfolio level. This paradigm would provide a predictable stream of adequate funding to ensure adequate funding is available to support multi-increment developments as well as to upgrade and sustain fielded capability. Using this approach creates a budgetary limit, placing the burden on the program to define capabilities that can be fit into those constraints (DSB, 2009, p. 52). Effective oversight can be maintained through the more thorough pre-planning stage, along with periodic milestone reviews. If one program is struggling to contain costs or is encountering technical challenges, funding can be reallocated at the discretion of the program executive.

In addition, "color of money" restrictions between capital and O&M accounts can prevent program management from responding to unforeseen situations by making trade-offs among internal milestones and priorities in order to achieve overall cost, schedule, and performance objectives.

Industry Cooperation

To achieve the ideal balance and control costs in the face of changing requirements will require that DoD programs engage industry as partners in the new process. During the acquisition of IT, requirements generally evolve during the development process, with only a small number of mission-critical big-R requirements being prescribed at the program's inception. The current acquisition process does not facilitate this evolution of requirements. On the contrary, the process strongly discourages changing requirements after Milestone B is reached. Acquisition teams must take better advantage of industry's understanding of technology alternatives and advances by collaborating with industry during the requirements development process. Government procures products and services from industry when industry is best suited to perform the required functions. This collaboration will help to clarify requirements, minimize the number of questions, and ultimately lead to better solutions being developed by industry.

Competition

The DoD must maintain the potential for competition throughout the *IT 360* cycle while rewarding outstanding results (performance, cost, and schedule) with follow-ons. Rewarding outstanding firms while at the same time maintaining the option for competition will require informed decision-making and even-handedness. Often, in an effort to enhance competition, firms that regularly achieve superior results (in terms of performance, cost, and schedule) are required to recompete purely for competition's sake. This is an unnecessary burden for firms with proven records of accomplishment.

There are several measures that programs should take to ensure that the potential for competition is not unnecessarily constrained. Using an open architecture and commercial standards will facilitate potential competition during each evolutionary cycle, since proprietary constraints can restrict the entry of competing firms that would then have to start from scratch. Further, customization of COTS software often leads to increased software maintenance and personnel costs, software update complications, and potential roadblocks to contract recompetition. At a minimum, customization will require developing a specific software patch every time the COTS software is updated.

Disciplined Requirements

Within the DoD, there is a strong aversion to partial solutions. Often, requirements capabilities are not assigned to future increments; rather, they are front-loaded onto the initial requirements document. By adopting *IT 360*'s evolutionary approach to acquisition, essential technologies can be fielded in the near term by delaying the instantiation of more time-intensive, costly, or technically challenging capabilities, some of which may, in fact, prove unnecessary. However, the new process is not immune to the premature inclusion of requirements. Program personnel should strive for well-defined objectives, but not over-defined requirements, for the initial increment.

Additionally, specifying unique requirements will drive up the cost of programs that use COTS products. Therefore, program personnel should shape their requirement to fit the capabilities and processes of the COTS products, and not the other way around. This will help to minimize customization of commercial products as well as benefit from the commercial best practices embedded in the software. For the new process to be successful, program personnel must adopt a disciplined approach towards requirements.

Maintain IT Security

The 21st century has brought together a variety of factors that have heightened the need for improving the DoD's IT systems security. First, the DoD is increasingly dependent on efficient business operations, almost all of which are IT-based. For example, current supply chain strategies (e.g., lean, just-in-time) reduce operating costs but can create new security vulnerabilities. Moreover, modern, "world-class" logistics systems (e.g., Wal-Mart, FedEx, Caterpillar, GE, etc.) are all IT-based. But cyberspace is no longer a protected domain; rather, it exists within the global commons and is accessible to virtually anyone with the requisite knowledge. It is not surprising, then, that cyber attacks have begun to play a larger role in modern warfare. One need only to look at Russia's recent use of a combination of cyber and kinetic attacks in its conflict with Georgia. The DoD's IT systems are not immune; recently, General Keith Alexander, the commander of U.S. Cyber Command, asserted that DoD systems

are “probed by unauthorized users approximately 250,000 times an hour, over 6 million times a day” (Lawson, 2010, p.1).

The increased use of COTS software that is envisioned under *IT 360* presents some unique challenges. With commercially developed software, DoD employees may be less familiar with the computer in question, which could lead to poor management and decision-making. Additionally, since many of these commercial software products are large and complex, they often comprise millions of lines of source code. This level of complexity makes it exceedingly difficult to detect all security threats.

Workforce

The last challenge relates to the quantity, quality, and culture of the DoD acquisition workforce. The DoD’s acquisition workforce has been downsized significantly over the course of the last two decades, which has led to a marked reduction in the DoD’s internal technical competencies. Approximately 63% of today’s government IT acquisition workforce are 45 years of age or older, and many lack the specialized skills of the younger generation. While private-sector contractors have a role and must continue to support the acquisition of IT systems, it is clear that the DoD must work to rebuild its acquisition workforce to ensure that it has the requisite ability to control the development of its information systems. This will require significant and specific action on the part of government. Priorities should include increasing government workforce agility, developing and enhancing human capital, and providing leadership stability to ensure program continuity.

Most of the legacy personnel and organizations have years of experience developing requirements-driven, specification-constrained, custom-designed and -built components and systems. The new process will substantially change the skills needed to effectively manage delivery of information capabilities. Under *IT 360*, they will need to incorporate constantly evolving, market-driven commercial systems. In many cases, this fundamentally changes the work that these personnel perform. The new workforce will need to cultivate a significant familiarity with the IT marketplace and technology trends, knowledge of cybersecurity, a strong understanding of user needs and priorities, the ability to perform trade-off assessments between

alternative strategies for implementing needed capabilities, the capacity to actively manage risk, and the skills necessary to create capability and investment road maps.

In short, for *IT 360* to be successful, the DoD must employ an appropriately trained, educated, and experienced acquisition workforce. The DoD must make changes with regard to how it handles recruitment, retention, and rotation (between government and industry). In addition, it must overhaul its acquisition education and training curricula so that it is aligned with the realities of today's IT priorities.

Barriers

There are a number of barriers to implementation, which must be removed in order to successfully implement the new process. These barriers are in the form of laws and regulations that were written by Congress to improve oversight over the Defense Acquisition System; many of them are imbedded in the NDAA, specifically in titles 10, 31, and 40 of U.S.C. Portions of these laws may have to be changed to fully implement *IT 360* as envisioned.

Research and Development Reporting

The NDAA continues to require that all R&D funds used for programs be submitted to Congress at "the start of the program" (NDAA, 2010). This regulation is intended to ensure that R&D funding is accounted for and that oversight is adequately provided. However, given the evolutionary nature of *IT 360* and the fact that many programs within a portfolio may benefit from the same R&D, reporting should be completed on an incremental or portfolio-level basis.

MAIS Reporting Thresholds

MAIS reporting procedures have been codified in multiple laws over time. As mentioned previously, MAIS programs are subject to more rigid reporting standards compared to non-MAIS programs. More specifically, 10 U.S.C. 2445(a) establishes MAIS cost thresholds that ultimately require program-based reporting and cost analysis. Because defense business systems often meet MAIS cost thresholds and are thus classified as such, defense business systems acquired via *IT 360* may be subject to the MAIS reporting process. This process hinders

acquisition because it does not facilitate incremental development. 10 U.S.C. 2445(a) should include provisions that allow for portfolio-level reporting for MAIS defense business systems.

Designated DoD Authorities

The designation of authority for all DoD acquisitions is established by Congress to ensure that oversight is properly applied to DoD programs. 10 U.S.C. 2222–2223 and 40 U.S.C. 11315 designate different authorities to oversee what were once discrete processes embedded within the traditional acquisition system. For example, the authority of investment review boards to analyze the strength of DoD investments was separate from that of the chief information officer who was responsible for ensuring product integration. As a result, there is ambiguity with regard to which oversight body holds the decision-making authority at certain points within the new process. Unless a change is made, oversight may be applied inconsistently. The previously mentioned statutes should be amended to clarify roles and create new ones, including, most notably, functional portfolio managers.

Specified Appropriations

Under the *IT 360* approach, requirements may be added or altered after the budget cycle has completed without increasing the level of programmatic risk. Indeed, flexibility is one of the key attributes of the *IT 360* process. However, this flexibility is jeopardized because 31 U.S.C. 1301 requires that all funds appropriated by Congress be used only for the programs and purposes for which the appropriation was made.

The current system's PPBE process, described in Section II, incorporates this congressional mandate and, thus, presents challenges to the efficient acquisition of IT. Specifically, Congress appropriates funding based on programs and appropriations categories (e.g., RDT&E; procurement). This allocation scheme can be problematic if, for example, a program is allocated more than enough for development but needs to fund additional testing. As previously mentioned, under the current system, reallocation of funds among phases is impermissible. Furthermore, the budget component of the PPBE process requires a three-year lead-time—even obtaining "reprogramming authority" (within low levels of funding) is very time-consuming.

With an 18-month change cycle, delays of this sort significantly reduce the potential for the successful implementation of a highly functional information system. Data standards, cybersecurity standards, and common industry-based protocols all change at regular intervals. Rigid budgetary constraints inhibit the integration of these new protocols and standards across programs. The appropriations cycle should be tailored to IT acquisition—and not vice versa. Funding through congressionally specified appropriations should be eliminated in favor of a regulation that codifies portfolio-level funding for IT programs.

VI. Conclusion

The DoD's current approach to IT acquisition is unable to deliver capabilities in a timely, cost-efficient manner. As the DoD works to improve its acquisition process for its IT systems, it must also contend with rapid technological change and a difficult economic environment in which budget pressures continue to mount. To achieve these objectives, the DoD must find ways of making the acquisition process deliver IT capabilities faster and more effectively. This report provides an alternative approach that can assist the DoD in accomplishing that goal.

Our review of various reports, government documents, and proposed strategies revealed a number of common themes. Chief among these themes was that the new IT acquisition process must leverage the agility afforded by an incremental development approach, economies of software reuse, and the ubiquity of web-based commercial products. Building on these themes, we have developed *IT 360*, which, we believe, should replace the traditional one-size-fits-all approach (based on the acquisition of weapons systems) for the acquisition of defense business systems. The features of the new process—smaller increments, continuous testing, and iterative prototyping—will improve performance, increase efficiency, and reduce costs. We have also proposed a number of supporting initiatives that should be implemented to strengthen the process. These include the use of flexible funding and contracting mechanisms as well as the inclusion of end users throughout the process.

The Milestone Decision Authority currently has the flexibility to implement and use our proposed process with ACAT III programs. Over time, the use of *IT 360* can be extended to larger program categories (e.g., MAIS). However, in order for *IT 360* to reach its full potential, the DoD must clarify roles and oversight responsibilities. At the same time, the DoD must also work with Congress to make the required legislative changes with regard to funding and reporting.

Given the current budgetary environment and the increased political pressure to reduce defense spending, the DoD must improve the efficiency with which it develops, acquires, and fields IT

systems. But even in the absence of such pressure, the DoD has a responsibility to the taxpayers, and to our military forces, to provide world-class IT capabilities at a reasonable cost.

Reference List

10 U.S.C. 132–133.

10 U.S.C. 2222–2223.

10 U.S.C. 2445(a)–(c).

31 U.S.C. 1301.

40 U.S.C. 11317.

40 U.S.C. 11315.

Acquisition Solutions, Inc. (2009, August). *A proposed process for rapid acquisition of information technology*. Retrieved from http://www.acq.osd.mil/damir/2009%20Conference/Modernizing%20IT20Acq.pdf

Adams, R., & Eslinger, S. (2004). *Best practices for the acquisition of COTS-based software systems (CBSS)*. Paper presented at the Ground Systems Architectures Workshop, Manhattan Beach, CA.

Armour, P. (2002, November). Ten unmyths of project estimation: Reconsidering some commonly accepted project management practices. *Communications of the ACM, 45*, 15–18.

Association for Enterprise Information. (2010). *Industry perspectives on the future of DoD IT acquisition*. Arlington, VA: Author.

Beck, K. (2003). *Test-driven development by example.* Boston, MA: Addison-Wesley.

Cai, Y., Ghali, S., Giannelia, M., Hughes, A., Johnson, A., & Khoo, T. (2004, June). Identifying best practices in information technology project management. *Project Management World Today*. Retrieved from http://www.pmworldtoday.net/

Chapin, J. (2004, September). The future of JTRS and its SCA: Lessons from ADA. *COTS Journal*. Retrieved from http://www.cotsjournalonline.com/articles/view/100190

Clinton, W., & Gore A. (1997). A framework for global electronic commerce. Retrieved from http://clinton4.nara.gov/WH/New/Commerce/

Component acquisition executive (CAE). (2011, July). In *Glossary of defense acquisition acronyms and terms* (14th ed.). Retrieved from https://dap.dau.mil/glossary/Pages/Default.aspx

Czelusniak, D. (1998, June 12). Defense Science Board Briefing. Washington, DC.

Defense Acquisition Performance Project Panel. (2006). *A report by the assessment panel of the Defense Acquisition Performance Assessment project for the Deputy Secretary of Defense: Defense acquisition performance assessment report.* Washington, DC: Department of Defense.

Defense Acquisition University (DAU). (2011, June). *Defense acquisition guidebook*. Retrieved from https://dag.dau.mil/

Defense Science Board. (2009, March). *Department of Defense policies and procedures for the acquisition of information technology.* Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics.

Department of Defense (DoD). (2010, November). *A new approach for delivering information technology capabilities in the Department of Defense* (Report to Congress). Washington, DC: Office of the Secretary of Defense.

Drezner, J., Raman, R., Blickstein, I., Ablard, J., Bradley, M., Eastwood, B., Falvo, M., Gavrieli, D., Hertzman, M., Lenhardt, D., & McKernan, M. (2006). *Measuring the statutory and regulatory constraints on DoD acquisition.* Santa Monica, CA: RAND.

Gallagher, S. (2010, August 10). Air Force lays foundation for strong cyber defense. (2010, August). *Government Computer News*. Retrieved from http://gcn.com/articles/2010/08/12/interview-maj-gen-richard--webber-commander-24th-air-force.aspx

Gansler, J., & Lucyshyn, W. (2009). *Defense business transformation*. Monterey, CA: Naval Postgraduate School.

Government Accountability Office (GAO). (2008). *Information technology: OMB and agencies need to improve planning, management, and oversight of projects totaling billions of dollars* (GAO-08-1051T). Washington, DC: Author.

Government Accountability Office (GAO). (2009). *DOD needs to strengthen management of its statutorily mandated software and system process improvement efforts* (GAO-09-888). Washington, DC: Author.

Government Accountability Office (GAO). (2010). *DoD business transformation: Improved management oversight of business system modernization efforts needed* (GAO-11-53). Washington, DC: Author.

House Armed Services Committee (HASC). (2010, March 23). *Panel on defense acquisition reform findings and recommendations* (Report to Congress). Retrieved from http://seaonline.org/AboutSEA/news/NewsDownloads/DARFINALREPORT032310.pdf

IT Acquisition Advisory Council. (2010). *A roadmap for sustainable IT acquisition reform: Congressional summary.* Arlington, VA: Author.

Jackson, W. (2011, February). DoD's Lynn: Public/private partnership key on cyber warfare. *Defense Systems*. Retrieved from http://defensesystems.com/articles/2011/02/16/rsa-6-lynn-dod-cyber-defense.aspx

Johnson, J. (2002). *Standish group study report for XP2002*. Presented at XP2002 Conference, Alghero, Sardinia.

Kundra, V. (2010, September 20). Remarks by Vivek Kundra, U.S. Chief Information Officer, Federal CIO Council. Washington, DC.

Kundra, V. (2011). Federal cloud computing strategy. Retrieved from http://ctovision.com/wp-content/uploads/2011/02/Federal-Cloud-Computing-Strategy1.pdf

Lapham, M., Williams, R., Hammons, C., Burton, D., & Schenker, A. (2010, April). *Considerations for using agile engineering in DoD acquisition* (CMU/SEI-2010-TN-002). Pittsburgh, PA: Software Engineering Institute.

Lawson, S. (2010). Just how big is the cyber threat to the Department of Defense? *Forbes*. Retrieved from http://www.forbes.com/sites/firewall/2010/06/04/just-how-big-is-the-cyber-threat-to-dod/

Moore, G. (1965). Cramming more components on integrated circuits. *Electronics*, *38*(1).

Nakashima, E. (2011, December). Cyber-intruder sparks massive federal response—And debate over dealing with threats. *The Washington Post.* Retrieved from http://www.washingtonpost.com/national/national-security/cyber-intruder-sparks response-debate/2011/12/06/gIQAxLuFgO_print.html

National Defense Authorization Act (NDAA) for Fiscal Year 2010, H.R. 2647, 111th Cong. (2010).

National Research Council. (2010, June). *Achieving effective acquisition of information technology in the Department of Defense.* Washington, DC: National Academy of Science.

Schwartz, M. (2009, June). *Defense acquisitions: How DOD acquires weapons systems and recent efforts to reform the process* (CRS 7-5700). Washington, DC: Congressional Research Service.

Strategy Page (2011, June 21). The Wormworm that won't die. Retrieved from http://www.strategypage.com/htmw/htiw/20110621.aspx

TechAmerica Foundation. (2010, July). Government technology opportunity in the 21st century. Retrieved from http://www.techamericafoundation.org/gto21

The Standish Group. (1995). The Chaos Report. Retrieved from http://www.csus.edu/indiv/v/velianitis/161/ChaosReport.pdf

Under Secretary of Defense for Acquisition, Technology and Logistics (USD[AT&L]). (2007, November 20). *The defense acquisition system* (DoD Directive 5000.01). Washington, DC: Author.

Acknowledgements

This research was sponsored by the Naval Postgraduate School. The authors are especially grateful to Rear Admiral Jim Greene (USN, Ret.), Keith Snider, and Keith Seaman for their encouragement, guidance, and support. We would like to thank Lt. General Ron Kadish (USAF, Ret.), former director of the Missile Defense Agency, and the Honorable Mike Wynn, former Secretary of the Air Force, for their review of our proposed process. We would also like to thank the Honorable Art Money, the former Assistant Secretary of Defense for Command, Control, Communications and Intelligence, for his review of our process and final report.

We would like to acknowledge Jeffrey Toor and David Ziman, graduate students in the School of Public Policy at the University of Maryland, whose research contributed to this report. Finally, we want to thank our co-worker Caroline Dawn Pulliam for her assistance with the planning and coordination of this study and faculty research assistant John Rigilano for his assistance with the editing of the report.

About the Authors

Jacques S. Gansler

The Honorable Jacques S. Gansler, former Under Secretary of Defense for Acquisition, Technology, and Logistics, is a professor and holds the Roger C. Lipitz Chair in Public Policy and Private Enterprise in the School of Public Policy, University of Maryland. He is also the director of the Center for Public Policy and Private Enterprise. As the third-ranking civilian at the Pentagon from 1997 to 2001, Gansler was responsible for all research and development, acquisition reform, logistics, advance technology, environmental security, defense industry, and numerous other security programs. Before joining the Clinton Administration, Gansler held a variety of positions in government and the private sector, including Deputy Assistant Secretary of Defense (Material Acquisition), Assistant Director of Defense Research and Engineering (electronics), Executive Vice President at TASC, Vice President of ITT, and engineering and management positions with Singer and Raytheon Corporations.

Throughout his career, Gansler has written, published, testified, and taught on subjects related to his work. He is the author of five books and over 100 articles. His most recent book is *Democracy's Arsenal: Creating a 21st Century Defense Industry* (MIT Press, 2011). In 2007, Gansler served as the chair of the Secretary of the Army's Commission on Contracting and Program Management for Army Expeditionary Forces. He is a member of the Defense Science Board and the Government Accountability Office Advisory Board. He is also a member of the National Academy of Engineering and a fellow of the National Academy of Public Administration. Additionally, he is the Glenn L. Martin Institute Fellow of Engineering at the A. James Clarke School of Engineering, an affiliate faculty member at the Robert H. Smith School of Business, and a senior fellow at the James MacGregor Burns Academy of Leadership (all at the University of Maryland). From 2003–2004, Gansler served as interim dean of the School of Public Policy. From 2004–2006, he served as the vice president for research at the University of Maryland.

William Lucyshyn

William Lucyshyn is the director of research and a senior research scholar at the Center for Public Policy and Private Enterprise in the School of Public Policy, University of Maryland. In this position, he directs research on critical policy issues related to the increasingly complex problems associated with improving public-sector management and operations and with how government works with private enterprise.

Current projects include modernizing government supply-chain management, identifying government sourcing and acquisition best practices, and analyzing Department of Defense business modernization and transformation. Previously, Lucyshyn served as a program manager and the principal technical advisor to the director of the Defense Advanced Research Projects Agency (DARPA) on the identification, selection, research, development, and prototype production of advanced technology projects.

Prior to joining DARPA, Lucyshyn completed a 25-year career in the U.S. Air Force. Lucyshyn received his bachelor's degree in engineering science from the City University of New York and earned his master's degree in nuclear engineering from the Air Force Institute of Technology. He has authored numerous reports, book chapters, and journal articles.

The Center for Public Policy and Private Enterprise provides the strategic linkage between the public and private sector to develop and improve solutions to increasingly complex problems associated with the delivery of public services — a responsibility increasingly shared by both sectors. Operating at the nexus of public and private interests, the Center researches, develops, and promotes best practices; develops policy recommendations; and strives to influence senior decision-makers toward improved government and industry results. The Center for Public Policy and Private Enterprise is a research Center within the University of Maryland's School of Public Policy.