UMD-AM-12-182

# Implementing System-of-Systems Governance

By:

Jacques S. Gansler, William Lucyshyn, and John Rigilano

Center for Public Policy and Private Enterprise
School of Public Policy

August 2012

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

University of Maryland 1856

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

The growth in new technologies, especially within the domain of information networking, has given rise to the desire to create tightly connected operational systems in order to improve task efficiency. This desire has become a driving force within both the private and public sectors. The DoD, for its part, has developed a strategy known as Net Centric Warfare (NCW), which envisions the translation of information superiority into combat power through the effective linking of "knowledgeable entities" within a given battlespace (Alberts, Garstka, & Stein, 2000). Individual assets are able to access information in real time, without having to navigate through disparate and disconnected information conduits, allowing them to more quickly assess and respond to situations.

To facilitate the greater level of integration that NCW required, an innovative DoD acquisition strategy arose: system-of-systems (SoS) development. SoS views the constellation of military assets in an integrated and coherent way—as a complete, interconnected system. The *Defense Acquisition Guidebook* (Defense Acquisition University, 2011) defines a an SoS as "a set or arrangement of systems that results when independent and useful systems are integrated into a larger system that delivers unique capabilities" (p. 1.4). These new capabilities can be derived from the integration of new systems, legacy systems, or a combination of both. Currently, however, the DoD's culture, practices, and management structure, are aligned with the acquisition of individual systems—and not with the acquisition of integrated systems-of-systems.

In general, DoD systems are designed, developed, procured, managed, reviewed, budgeted, and supported on an individual basis. Although this acquisition structure, developed over the past half century, has produced some of the most advanced weaponry in the world, it has significant drawbacks. For example, the historic development of single platforms (e.g., ships, aircraft, etc.) has placed a premium on performance—producing the best weapon system attainable—as opposed to considering the potentially complementing capabilities of other systems in the DoD arsenal or those under development.

In the SoS environment, this legacy governance structure is a growing liability—not only must each DoD program's personnel have knowledge of other systems across the range of DoD

programs, but they must also work to actively integrate these systems. Moreover, attempting to optimize each element of an SoS can, in fact, produce a suboptimal result. In order to create operational systems that are tightly coupled, they should be viewed, managed, and acquired as an SoS. However, the DoD's transition to SoS will not be without its challenges. For the majority of their history, the military forces have operated within their own domains (i.e., land, sea, and sky), and each Service has its own core mission, derived primarily from the environment in which it operates.

Current governance structures are unable to adequately assess and mitigate the risks that occur within the SoS environment. The DoD is organized hierarchically, and the program governance system is, likewise, hierarchical. Policies, regulations, and directives flow vertically, with few horizontal interactions. Moreover, authority is often segmented with different Services overseeing projects within their respective domains. At lower levels, program managers oversee the acquisition of individual weapons and systems to include their development, testing, repair, and disposal. Unfortunately, hierarchical structures are not well-suited to the SoS environment, which, in theory, takes the form of "a web of shared interests" rather than a hierarchical chain of command (Morris, Place, & Smith, 2006).

Despite the rigidity of existing governance structures, program managers have successfully injected some flexibility into the system by, for example, organizing teams in ad hoc fashion to work on program-specific tasks that are not formalized within the standard governance structure. In fact, the DoD has implemented initiatives over the last couple of decades, such as integrated product teams (IPTs), to facilitate this tendency among managers. An IPT consists of a small group of cross-functional, multidisciplinary members, dedicated to a specific task. Regrettably, this level of organizational integration does not often exist at the higher levels within the DoD's governance structure. As a result, the decision to, for example, modify one system is often made in isolation, even though it will invariably have an impact on other systems within the DoD's inventory of systems.

As John Dillard (2008) points out, the IPT philosophy has also come to inform command and control tactics as well, with emphasis being placed on transmitting essential information to the "tactical edge." Both on and off the battlefield, the DoD has begun to recognize the advantage of

empowering lower level personnel in order to "transfer knowledge and power to the point of an organization's interaction with its environment" (Dillard, 2008, p. 261). Research in organization theory (e.g., Engwall, 2003; Thomas & Buckle, 2004) supports the DoD's move to decentralize control, via the empowerment of lower level entities.

However, decentralization is no panacea, especially with regard to SoS; in fact, it can be a considerable liability. Whereas a decentralized approach may work well when acquiring a typical system consisting of highly defined subsystems and components (e.g., an aircraft), the same cannot be said for novel SoS with evolving requirements. SoS governance requires collaboration and integration across programs and assets. Decisions and trade-offs need to be made at levels higher than the individual system. The distributed ownership of individual systems creates a problem that governance mechanisms must be designed to address. Without adequate mechanisms, project managers will develop their systems in accordance with their localized priorities, which will compromise the efficiency and effectiveness of the SoS (Morris, Place, & Smith, 2006).

We contend that all SoS can be governed using similar mechanisms, and that it is merely the extent to which these various governing mechanisms are applied that will vary. One of the fundamental goals of SoS governance is to map a trajectory along which the program in question can grow and evolve. However, there is no single best SoS governance structure. In fact, the most successful regimes are, to a great extent, self-organizing. The ideal structure will draw on a variety of governance mechanisms in order to facilitate a flexible strategic process (Miller & Hobbs, 2005). The structure may incorporate characteristics of different governance regimes, including markets, contracts, hierarchies, budgets, and associations (North, 1990; Miller & Hobbs, 2005).

The challenge of SoS governance is achieving a balance: directing growth via firm protocols so as to avoid functional redundancies and component optimization (as opposed to system optimization) without stifling the emergence of unanticipated (though desirable) linkages and emergent behaviors. This will require incisive decision-making. When SoS programs are unbalanced, problems occur. On the one hand, programs exhibiting an overreliance on open architectures may suffer from a lack of upfront systems engineering. Program personnel may

assume, incorrectly, that an open systems architecture, which is responsive by nature to changes in technology and is flexible in design to accommodate technological advances in software and hardware, may obviate the need for upfront engineering, planning, and deliberate integration. Systems-of-systems are intended to have wide-ranging impact, from platforms to organizational structures, training, tactics, and doctrine. Thus, from a decision-making perspective, it is critical to understand how the different elements of the program will interact, to ensure the optimal level of integration and interoperability for mission effectiveness.

Military leaders must take into account the unique characteristics of each SoS program in establishing a governance structure. That said, certain elements of SoS governance can be discussed generically. For instance, all SoS programs must dedicate resources to establishing a management strategy, defining requirements, providing oversight, ensuring integration, and obtaining funding. From the theoretical perspective, these mechanisms of SoS governance should be similar, at least in some respects, across programs. For example, program managers must have visibility over the entire range of constituent systems, because decisions made about individual components or systems will have ripple effects on the other elements within the system. In addition, programs must be able to translate envisioned capabilities into specific system requirements. To ensure integration, the governance structure must be able to determine which elements of the SoS should be modified, who is responsible to oversee the work, and, in a multiple program environment, which office's budget will cover the costs.

In order to determine how actual governance contrasts with these theoretical considerations, we examine three SoS programs: the Coast Guard's Integrated Deepwater System Project, the Joint Tactical Radio System, and the Army's Future Combat Systems.

Interoperability was the driving force behind the U.S. Coast Guard's (USCG) modernization effort known as Deepwater. The USCG selected a private-sector lead systems integrator (LSI), chosen from multiple bids, to lead the development project. However, the USCG did not have the necessary human capital and technical ability to manage or even oversee the management of such a complex project. In addition, the failure to use specific language with regard to contracts and requirements proved disastrous. For instance, task orders for specific outputs "did not identify which party had decision-making authority over structural design specifications; the

conditions under which third-party assessment of the design would be necessary, or which organizations would be qualified to perform this role" (Brown, Potoski, & Van Slyke, 2008, p. 33). In 2007, the USCG officially assumed LSI duties.

The Joint Tactical Radio System (JTRS; pronounced "jitters") was initiated by the DoD in 1997. JTRS was a transformational communications network that was designed to allow warfighters and support personnel to seamlessly transmit voice, picture, and video via a high-capacity, wireless network. Since the program's inception, however, DoD officials have consistently overestimated the ease with which various components of JTRS could be developed and implemented. There was no enterprise-wide systems engineering master plan. Accordingly, each radio was designed to meet Service-specific needs and desires with little regard for how the radio might fit within the overall network or integrate into different platforms. This has resulted in a program that has experienced delays, unforeseen technical hurdles, and major cost overruns.

The Army's Future Combat Systems (FCS) project was the "Army's first full-spectrum modernization in nearly 40 years" (U.S. Army, 2007). FCS originated as the combat portion of the Army's 2003 planned Future Force, the overarching strategy to prepare the Army for operation in the next century. The Army granted the prime contractor, Boeing, SoS integration responsibilities. Ultimately, the Army believed FCS would support NCW and offer the Service a force that is more responsive, more integrated, and more sustainable than its current force. However, the program was canceled in 2009 because of technical difficulties, major cost overruns, and the belief, at least among DoD leadership, that the program was poorly aligned with modern military objectives. Indeed, the wars in Iraq and Afghanistan presented the Army with a need for new, unanticipated capabilities that, even when fully fielded, FCS would be unable to provide.

There are a number of challenges to successful SoS governance. These challenges fall into five categories: leadership, management, requirements, human capital, and funding. We describe these challenges in the following bulleted list.

- **Frequent leadership changes lead to program setbacks.**

  Frequent changes in senior leadership can lead to significant changes in an organization's priorities, goals, and strategy. These changes can also significantly impact relationships with partnering organizations.

- **Ineffective intergroup leadership inhibits collaboration.**

  When personnel are also assigned to cross-functional teams composed of individuals from different programs—and possibly from different military Services and agencies—they may not recognize the importance of achieving successful outcomes, even if (perhaps especially if) the task involves the integration of different programs' systems.

- **SoS vision statements change over time.**

  Vision statements change radically over time. This is attributable to frequent leadership changes, but also to rapid improvements in technology (especially within the commercial sector) and a changing battlefield environment.

- **Managers of individual programs are not incentivized to ensure system-wide integration.**

  A good program manager works to develop system capabilities as cost effectively as possible, but because funding is appropriated to individual systems that are under the authority of different offices, there is often no incentive on the part of individual program offices to integrate these capabilities with those of other systems, particularly when integration costs are high, but the benefit is less obvious at the program level.

- **Management does not reward local interventions.**

  Project personnel working closely on a particular facet of a program rarely intervene to prevent potential system problems. In fact, intervention is often regarded as symptomatic of an earlier failure to properly plan and execute the project.

- **SoS requirements are often overly ambitious.**

  Program decisions to begin design and/or production are made without sufficient knowledge. As a result, requirements tend to be overly ambitious, and, thus, unachievable.

- **SoS requirements are constantly modified.**

  Requirements modification is especially problematic within the SoS environment. Adding, cancelling, or changing requirements has an impact on other constituent systems.

- **Platform design is not given adequate consideration.**

  In the SoS environment, the DoD's focus is on capabilities and objectives, often to the exclusion of platform design and integration. In some instances, it seems, capabilities are conceptualized in the abstract, untethered from the equipment upon which they rely.

- **The DoD's workforce does not have the capacity to oversee complex SoS programs.**

  Currently, the DoD does not have the technical or managerial capability to oversee private-sector providers of complex SoS (increasingly, combining manned and unmanned systems, often multi-Service, and multinational).

- **Retaining high-quality managers is challenging.**

  Hiring and retaining skilled personnel with experience managing complex programs is essential to the success of the DoD's SoS programs. However, highly qualified individuals tend to gravitate toward the private sector, because the compensation is higher.

- **Funding is appropriated to individual systems.**

  In general, there is no single funding source for systems-of-systems. As a result, there is no advocate for joint or, as the case may be, enterprise-wide capabilities.

- **Funding is inflexible.**

  Even in instances when a central authority is tasked with allocating funds among different systems, funding is rarely reallocated in response to changes brought on by the SoS program's evolution

Given the number of organizational permutations that are possible, it is impractical to develop a single governance model. However, based on our theoretical discussion of systems-of-systems, the literature on the governance of complex projects, and our examination of past SoS programs, we can outline a notional governance structure, its attributes, and its composition.

A basic structure might consist of two levels. The lower level would be composed of individual program office officials, along with user representatives and other stakeholders. As one might expect, many program-level functions (e.g., systems engineering, logistics, and test and evaluation) must also be performed at the level of the SoS. This group would be tasked with coordinating these functions. In addition, this group, which we will term the Integration Working Group, identifies problems as they arise and proposes solutions that are then implemented by the appropriate program office. In the event that the issue cannot be resolved, or if consensus is not obtained, the problem is elevated to the upper level for adjudication. We will term this level the Senior Leadership Board.

The Senior Leadership Board would be led by the program executive officer (PEO), who is responsible and accountable for delivering the envisioned capabilities of the SoS. The other members include program managers of the constituent systems, senior user representatives, and other appropriate stakeholders. The Board would be responsible for maintaining the requirements baseline—restraining the natural tendency to make the program "better"—as well as allocating funding among the different programs. As the SoS evolves, and requirements change, ensuring

systems integration becomes critical. The Board would be tasked with deciding which element(s) of the SoS should be modified and how those changes are to be resourced.

Program leadership must walk a fine line; it must provide a conception of the SoS that is visionary, yet practical. We believe that the following recommendations, once implemented, will help leadership to achieve the correct balance.

- **Provide stable leadership.**

  To the degree possible, program continuity should be ensured, especially with regard to key senior leadership. Political appointees can be especially critical for high-profile systems-of-systems. To have a lasting impact on SoS programs during their short tenure, they must assume their role quickly.

- **Develop intergroup leadership and collaboration.**

  Senior leaders must continuously emphasize to members of the Integration Working Group and the Senior Leadership Board that collaboration is essential to achieving outcomes that are deeply valued by their respective organizations (Hogg, van Knippenburg, & Rast, 2012).

- **Ensure requirements stability by using an evolutionary approach.**

  Initial requirements should remain fixed in the short term. The first increment of an SoS program must be designed, produced, and fielded so as to offer useful capabilities to the warfighter in a timely manner. By adopting an evolutionary approach, the SoS Senior Leadership Board can maintain the requirements baseline without sacrificing the long-term SoS vision, for which it is also responsible.

- **Verify SoS integration.**

  In order to map out an efficient trajectory along which the SoS can evolve, the Integration Working Group should promote the use of architectural tools and prototypes. These tools

can be used to anticipate unexpected couplings and avoid the potential for overlooked, underutilized, or duplicated functionalities.

- **Strengthen human capital.**

  At present, the DoD does not have the capacity to oversee SoS programs. The DoD must recruit highly qualified systems engineers who have relevant domain experience to manage and oversee SoS programs. However, staffing all programs internally is simply unrealistic. Accordingly, the DoD should continue to rely on private-sector firms for their systems engineering and integration expertise, provided that there is adequate government oversight, and conflict-of-interest issues are explicitly addressed.

- **Provide greater funding flexibility.**

  Providing funding at the platform level tends to facilitate system (as opposed to SoS) optimization. The Program Leadership Board must be able to allocate and divert funding among individual programs in order to promote the objectives of the SoS.

  This funding issue is particularly critical in a period of declining DoD resources. One advantage of the SoS approach is greater overall force effectiveness for fewer total dollars—when the SoS is configured and managed from the total-cost-effectiveness perspective. However, this requires flexibility in making design, funding, quantity, and performance trade-offs among the various elements of the SoS.

A robust SoS governance structure is necessary to coordinate requirements, budgets, schedules, and modifications in order to successfully deliver the end products. As the old saying goes, a chain is only as strong as its weakest link. Our modern adversaries view the U.S. military in much this way, working tirelessly to exploit its weaknesses using whatever means possible. Our armed forces must be able to adapt quickly in such an environment. By leveraging the benefits of integrated, interoperable systems (e.g., heightened situational awareness and seamless communication), the U.S. military will be able to successfully counter today's asymmetric threats.

# I. Introduction

The advances in information technology have enabled the integration of individual military weapon systems into a group of task-oriented resources that, when employed together, provide emergent capabilities. These new capabilities can be derived from the integration of new systems, legacy systems, or a combination of both. Rather than acquire individual systems platform by platform, the Department of Defense (DoD) can modernize a mission capability with a single, fully integrated SoS development approach. Currently, however, the DoD's culture, practices, and management structure, are aligned with the acquisition of individual systems—and not with the acquisition of integrated systems-of-systems.

In general, DoD systems are designed, developed, procured, managed, reviewed, budgeted, and supported on an individual basis. Although this acquisition structure, developed over the past half century, has produced some of the most advanced weaponry in the world, it has significant drawbacks. For example, the historic development of single platforms (e.g., ships, aircraft, etc.) has placed a premium on performance—producing the best weapon system attainable—as opposed to considering the capabilities of other systems in the DoD arsenal or those under development. Of course, this is understandable, even laudable, given the acquisition structure's lack of flexibility. But because managers of individual programs have been unable to make knowledgeable trade-offs between systems in order to reduce the number of overlapping requirements, acquiring needed capability at reasonable cost has become increasingly difficult, especially in today's resource-limited setting.

In the SoS environment, this legacy governance structure is a growing liability—not only must each DoD program's personnel have knowledge of other systems across the range of DoD programs, but they must also work to actively integrate these systems. Moreover, attempting to optimize each element of an SoS, can, in fact, produce a suboptimal result. If the objective is to field tightly coupled operational systems, then they should be viewed, designed, managed, tested, and acquired as an SoS.

An SoS consists of large-scale concurrent and distributed systems that are, themselves, comprised of complex systems (Kotov, 1997). Unlike a family of systems or product line (e.g., a family of aircraft, submarines, or missiles), SoS provide more functionality and overall mission performance than simply the sum of the constituent systems. For decades, it has been noted that technically sophisticated, organizationally and geographically dispersed systems are becoming more complex and more common in both the private and public sectors (Ivory & Alderman, 2005; La Porte, 1994; Perrow, 1984). Moreover, there is no indication that this trend will reverse. As the largest organization in the world, with its myriad agencies, functions, and systems, the DoD has a vested interest in maximizing the acquisition of SoS.

The confluence of five factors in particular demands that the DoD embrace the acquisition of SoS in the near term: (1) the DoD's military doctrine, Network Centric Warfare, envisions the linking or "networking" of virtually all battlefield entities in order to counter today's asymmetric threats; (2) the military is already resigned to replacing many of its aging assets that are reaching the end of their intended service; (3) military appropriations have begun to stagnate (or decline) on account of growing national budgetary constraints; (4) the likelihood that achieving total force effectiveness will require multiservice (joint) operations, as well as integrated, coalition (multinational) operations; and (5) the growing complementarity of manned and unmanned systems, operating together for increased total force effectiveness. It is clear that the development of cost-effective SoS is ideally suited to the current defense environment. But in order to ensure appropriate management of the unique risks and opportunities that SoS development presents, significant change is necessary. The technical aspects of SoS engineering, though obviously critical, must not overshadow the necessity of a well-functioning governance structure, without which the full potential of SoS cannot be realized.

## *Report Roadmap*

We begin by providing a brief historical background in order to contextualize the growing importance of SoS governance. Next, we contrast the shortcomings of traditional governance regimes with the necessary characteristics of an SoS regime. We then analyze prior attempts to acquire SoS, and the role that governance played in their successes and failures. Specifically, we

examine the Coast Guard's Integrated Deepwater System, the Joint Tactical Radio System, and the Army's Future Combat Systems. We discuss program challenges and articulate the lessons learned. Next, we identify specific challenges to effective SoS governance. Finally, we provide recommendations to overcome these challenges and offer what we believe to be the essential elements of a successful SoS governance structure.

# II. Background

In 1996 Admiral William Owens noted that "the things that give military forces their fighting capabilities are changing, and these changes point toward a qualitative jump in our ability to use military force effectively" (p. 1). Owens was referring to the rapid growth of technologies, especially within the domain of information networking. New technology has begun to revolutionize the way that the United States wages war. In particular, the military has come to rely on three evolving capabilities, described in the following bullet list.

- **Intelligence, Surveillance, and Reconnaissance**
  New sensor and reporting technologies allow for the advanced tracking of military forces.

- **Advanced Command, Control, Communications, Computer Applications, and Intelligence Processing**
  Sensor awareness is converted into a dominant understanding of the battlespace, which is then used to control the battlespace.

- **Precision Force**
  Knowledge of the battlespace allows military assets to destroy selected high-value and time-critical targets or to inflict damage with precision while limiting collateral damage.

The ability to apply precision force has proven essential. Since the end of the Cold War, the DoD has had to prepare for war within the context of a rapidly changing national security environment. The threat posed by traditional adversaries (i.e., nation-states) with large-scale conventional military force structures is less prominent than that posed by numerous non-state actors. Our new adversaries employ asymmetric approaches including terrorist and guerilla tactics. A new term of art—"war amongst the people"—has come to denote the reduced capability of traditional military forces to successfully employ force. In today's conflicts, "civilians are the targets, objectives to be won, as much as an opposing force" (Smith, 2005, p. 6). In an effort to adapt to this new environment, the U.S. military has integrated the three capabilities described above into a new strategy known as Network Centric Warfare (NCW).

The growth in new technologies has given rise to the desire to create tightly connected operational systems in order to improve task efficiency. This desire has become a driving force within both the private and public sectors. NCW, for its part, envisions the translation of information superiority into combat power through the effective linking of "knowledgeable entities" within a given battlespace (Alberts, Garstka, & Stein, 2000). It was believed that this linking or "networking" of virtually all battlefield entities would serve to accelerate "engagement cycles and operational tempo at all levels of the warfighting system" (Kopp, 2005, p. 3). NCW envisions many advantages over traditional warfighting methods. First, individual assets are able to access information in real time without having to navigate through disparate and disconnected information conduits, allowing them to more quickly assess and respond to situations. Second, complete battlefield awareness, along with advances in precision munitions, allow for far more accurate fire placement. Third, seamless information flow allows units to act as a cohesive whole, even when assets are geographically dispersed.

To facilitate the greater level of integration that NCW requires, an innovative acquisition strategy arose: SoS (SoS) development. SoS views the constellation of military assets in an integrated and coherent way—as a complete, interconnected system. Military planners believe that SoS development will allow for the concurrent acquisition of a number of complex programs that will function collectively in the NCW environment and exhibit emergent capabilities.

However, the DoD's transition to SoS will not be without its challenges. For the majority of their history, the military forces have operated within their own domains (i.e., land, sea, and sky). And, to this day, Title 10 of the *U.S. Code* dictates that the military's budgets are to be provided at the Service level. This funding structure serves as a basic acknowledgement that each Service has its own core mission, derived primarily from the environment in which it operates. However, interoperability, flexibility, jointness, and interdependency are the vocabulary used to describe complex SoS. In order to effectively acquire SoS, the military Services must, themselves, incorporate this vocabulary into their organizational cultures.

As Conant and Ashby (1970), pioneers in the field of cybernetics,[1] asserted some time ago, "every good regulator of a system must be a model of that system" (p. 89). Superficially, this assertion can be taken to mean, quite simply, that control requires resemblance. The more sophisticated interpretation, however, is also applicable: a regulator (in this case, a governance structure) that lacks a complete picture of the system in question, or that is only capable of articulating a simplified version (and even then only by way of reference to other components or abstract representations) cannot effectively control (i.e., govern) the system. Scholten (2012) provides an example of this type of failure occurring within the field of diagnostic medicine. He writes,

> "Evidence-based" medicine, with its insistence on treatments that have been confirmed by "well-designed, large-scale, double-blind, randomized, placebo-controlled, clinical trials" will almost always cripple a doctor's ability to model symptoms as they actually occur within the anatomically, physiologically, and biochemically specific context of a given patient. (p. 1)

Currently, the distributed ownership across the DoD of individual systems reinforces platform-centric acquisition practices—practices that inhibit the ability of management to view, let alone model (either physically or theoretically), its particular system within the context of the SoS. Managers rely on their past experiences, natural biases, and localized priorities, placing undue emphasis on processes or system features that fail to facilitate the successful development of the SoS.

In 1986, Congress passed the Goldwater-Nichols Act, which streamlined the military chain of command in order to better leverage the capabilities of a unified, joint force and put an end to inter-Service rivalry. But, many claim that more drastic changes may be necessary in order to ensure that interdependence is the rule, not the exception. In any case, it is clear that the DoD, in many cases, will have to alter its hierarchical, platform-centric acquisition governance structure.

[1] Cybernetics is the theoretical study of communication and control processes in biological, mechanical, and electronic systems, especially the comparison of these processes in biological and artificial systems ( "Cybernetics," 2009).

Individual program offices will have to relinquish some control over their programs, ceding it to different authorities, both within and beyond individual Service boundaries. Specific traditions and practices have shaped each Service over time. Accordingly, a change of this magnitude will likely encounter resistance.

## *SoS Defined*

The term system-of-systems lacks a clear definition for a number of reasons. First and foremost, the concept is still in its infancy. Second, the concept can be applied to many fields and professions—from biology and transportation to healthcare and defense. For the purposes of this report, we rely on the definition provided in the *Defense Acquisition Guidebook* (Defense Acquisition University, 20011), which defines an SoS as "a set or arrangement of systems that results when independent and useful systems are integrated into a larger system that delivers unique capabilities" (p. 1.4).

While there may be no commonly accepted definition, it is generally agreed that SoS have five key attributes (Sage & Cuppan, 2001).

1. **Operational Independence**
   An SoS is composed of systems that can be operated independently of each other. If the SoS were to be disassembled, each component part would continue to operate and be useful.

2. **Managerial Independence**
   The component systems maintain an operational independence, but possess the necessary knowledge to interact for a specific goal.

3. **Geographical Distribution**
   Each component is capable of interacting with another, even when geographically dispersed.

4. **Emergent Behavior**

   The SoS performs functions and carries out a purpose that cannot be achieved by an individual system. This is one of the principle purposes of constructing an SoS.

5. **Evolutionary Development**

   Development of an SoS is never complete, with structure, function, and purpose being added or removed over time.

## *SoS in Theory*

It is important to realize that virtually every entity to which we attach the label "system" can, in fact, also be referred to as a component within a larger system. And, conversely, what we once viewed as a component within a system may, in another context, come to be seen as a combination of several constituent systems within a larger one. As we ascend through ever larger systems-of-systems (of systems?), we find that this is recursively true at many levels. The following example illustrates this point.

> Imagine some hypothetical data systems that interoperate in some manner. These data systems could all be elements (e.g., communication or navigation) of a military aircraft's avionics system, which together with many other systems (weapons system, mission management system) compose the total aircraft, which itself can be viewed as a single system. To continue to even higher levels, the aircraft is an element in a larger system of systems, since it interoperates with other aircraft and other military units in combat (Carney, Fisherman, & Place, 2005, p. 3).

Indeed, many of the DoD's capabilities exist within an SoS, even if they are not explicitly recognized as such (Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics [OUSD(AT&L)]), 2007). No military asset acts in isolation; instead, each one operates as part of a larger whole. For example, a Navy carrier battle-group could be viewed as an SoS.

Components of the battle-group include the aircraft carrier, aircraft, supporting ships, satellite communications, and personnel. Each part of the group could function independently, but, when synchronized, the benefit is greater. A battle-group might also be viewed as part of a broader SoS, with multiple groups composing a fleet, or multiple fleets composing the naval amphibious forces. Additionally, other SoS participate with the Navy, such as intelligence and reconnaissance units, or systems within other branches of the military.

What, then, is the difference between "explicitly recognized" SoS and unrecognized SoS (e.g., Navy carrier battle-groups)? The "differentiating point" according to Sisti and Latimer (2007) is that the latter are, by their very existence, "precedented" (p. 74). That is, they address "a similar functionality developed earlier using older and less complex technologies" (Sisti & Latimer, 2007, p. 74). In this report, we focus on explicitly recognized, or unprecedented, SoS. For these SoS, there are no prior examples on which to base development. Not only is the functional capability unprecedented, but so is the internal organization of components and the relationships to external stakeholders and other systems.

As mentioned, the components, or constituent systems, within an SoS necessarily retain their operational independence; that is, they are capable of functioning within and apart from their parent SoS. If this were not the case, then the SoS construct would lose its meaning; for what, then, would differentiate between a system (of components) and a system-of-systems ? However, there are some important qualifications in this regard. First, the fact that a constituent system is capable of providing some utility outside of the SoS context does not mean that interdependencies do not exist. To the contrary, the more evolved an SoS is, the more dependent each system becomes (Allison et al., 2004). This is obviously true with respect to biological SoS. For example, each cell within the human body (a complex SoS, indeed) retains its operational and managerial dependence in order to complete specific tasks, all of which are subordinated to a larger purpose—the survival and reproduction of the human being. The constituent systems within the body have become highly interdependent as a result of evolution, to the point where the larger systems do not often survive if other large systems die (e.g., cell death is a regular occurrence having little impact on other bodily systems, but when a more complex system—say, the lungs—dies, other systems will cease to function).

Military and other man-made SoS are similar in this regard. As the complexity of the SoS increases, systems become more interdependent. A good governance structure can help anticipate some of these interdependencies, allowing military planners to make trade-offs between systems in advance, in order to improve cost efficiency and system effectiveness. When trade-offs are not prescribed and interdependencies evolve only in ad hoc fashion (as they do in the natural world), the costs may exceed the benefits, especially when this "blind" process engenders functional redundancy and, ultimately, noninteroperability. And, while redundancy is common in the natural world (e.g., plants that evolve both resistance *and* tolerance to drought or frost conditions), it is also costly and inefficient, which is why at the level of the individual organism, there is often a negative correlation between the two adaptations as a result of natural selection. The DoD, for its part, does not have the time, or money, to let nature simply take its course. Rather, it must strive to streamline the evolutionary process upon which it relies to acquire new capabilities. Ideally, military SoS would evolve only necessary capabilities and minimize redundancy—a difficult feat, indeed.

However, not all interdependencies, linkages, and behaviors can be anticipated in advance. The term emergent behavior, which has a long history in science and technology fields, is increasingly being used within the context of SoS. An emergent behavior of a system is behavior that cannot be predicted by a knowledge of the system's constituent parts (DeLaurentis & Crossley, 2005). Another analogy to biology seems apt. Humans' subjective experience of consciousness cannot be mapped on to the physical reality of the brain. Consciousness merely "arises" as a result of physical interactions that scientists cannot fully explain. Indeed, an SoS's emergent properties assure that the SoS offers still more functionality than the sum of its constituent parts. With regard to human consciousness, even if the various physical interactions were to be fully decomposed and articulated, there is no doubt that this would still be the case.

On the other hand, undesirable system behaviors, linkages, and interdependencies also occur and cannot be anticipated, thus, requiring costly system redesign. With this in mind, military leaders, program personnel, stakeholders, and even the general public must come to realize that large SoS programs are inherently high risk. That the DoD is regularly criticized—sometimes justifiably—

for exceeding program budgets may make selling SoS programs to Congress, not to mention the public, particularly challenging.

## *SoS Engineering*

SoS engineering (SoSE) and traditional engineering differ in several significant ways (see Table 1). The primary difference between traditional engineering and SoSE is with regard to the objective. The former sets out to optimize the performance of a single system, given specific end requirements. Once the system has reached the extent of its usefulness, a new entity will be developed to replace the current one. SoSE, on the other hand, pursues a different end goal: develop a certain capability, attainable through the integration of individual assets.

Whereas traditional engineering places emphasis on individual systems, by designing to a required mission capability, SoSE places emphasis on the collective ability of the system. Because of this shift in emphasis, SoSE encounters two unique challenges. First, an SoS has a theoretically infinite lifespan; they are "enduring even though the individual systems that comprise them have finite lifetimes" (Kaplan, 2006). In other words, a useful capability, such as an integrated communications network, can be maintained indefinitely through a continuous process to update old systems through new acquisitions. Second, an SoS has unbounded development requirements. Because the lifetime of a mission need may be infinite, and the program evolves over time, end requirements may not be fixed by a single design iteration.

| | **Traditional Engineering** | **SoSE** |
|---|---|---|
| Goal | Optimized system | Integrated mission capability |
| Lifetime | Specific design lifetime | Indefinite lifetime |
| Design Requirements | Bounded | Unbounded |
| Size | Single system | Multiple systems |
| Independent Developments | Rare | Common |

**Table 1. Differences Between Traditional Engineering and SoSE**
(Kaplan, 2006)

Traditional engineering relies on designing a "well-bounded system … predicated on having well-defined, precise, and stable requirements" (Stevens, 2004). Given exact performance standards, the engineers design a system to meet the desired specifications. SoSE, on the other hand, does not have a specific endpoint to design around. Lacking an endpoint, engineers are unable to optimize the performance capabilities of a single system. In effect, an unbounded set of development requirements exists. The flexibility of SoSE allows the individual systems and the SoS to adapt to the challenges of the future as they arise. In this way, SoSE avoids the design problem of traditional engineering: designing for the wrong problem or designing around the wrong set of system parameters.

In addition, independent innovation (see Table 1) is less likely to occur in the development of a single system that has clearly defined requirements. With a predetermined set of requirements, traditional engineering extensively plans development to bridge the gap of knowledge between what is achievable today and the project's end result. Independent innovation is much more likely to occur with the development of multiple systems with unbounded requirements. As the final endpoint is not known, SoSE fosters innovation that will derive new solutions across the entire SoS.

Despite these benefits, the grand, unifying, theory upon which SoSE rests has yet to be fully explored. SoSE is still a maturing discipline. Indeed, there is no comprehensive manual for practitioners. In 2008, the OUSD(AT&L) released its *Systems Engineering Guide for Systems of Systems,* which "raises awareness" of the issues, but in most instances, is unable to provide practical advice. Moreover, it is important to realize that many of the persistent challenges associated with SoSE are also common to traditional engineering. Such challenges are continually overlooked. For instance, in 1984 Perrow argued that when complex systems suffer catastrophic failure, there are usually multiple causes. More recently, he asserted that "the more 'tightly coupled' or less slack in the system the more prone to cascading failure and catastrophic consequence" (Perrow, 1999, p. 11). Ivory and Alderman (2005) attribute this failure to the number of interactions that characterize large systems. More specifically, they assert that these interactions can be linear or non-linear. Linear interactions, they write, "can be expected and even predicted, while non-linear interaction between parts or subsystems cannot be predicted by

the systems designer" (p. 6). Problematic interactions are either hidden from view, and, thus, undetectable, or they are ignored because they do not fit expectations of the system or its environment (Ivory & Alderman, 2005; Perrow, 1984). However, the relationship between complexity and failure is often ignored, because engineers, testers, developers, and program managers seek to attribute the failure to a single factor. In a similar vein, Sisti and Latimer (2007) assert that "the urge is for technical engineering personnel to simplify the problem to one they can solve" (p. 74). Although education and training may play a role in this regard, this way of thinking, is, more than anything else, a limitation of our collective psychology.

Extrapolating from Perrow's (1984) earlier analysis, it seems clear that SoS engineers will encounter a similar challenge, but on a much larger scale, in that non-linear interactions occur not only between "parts and subsystems," but between entire systems that, themselves, are composed of multiple components and subsystems. In any case, if systems failure can be attributed to the large number of interactions that characterize these systems, as the literature suggests, then SoS program governance must be designed to facilitate a multi-causal perspective when it comes to troubleshooting the technical problems that arise.

# III. Program Governance

Though the DoD is unique in that no organization, private or public, rivals it in terms of its sheer size or the breadth of its missions, the DoD might be compared to a large, multi-faceted corporation. In fact, in many respects, the DoD aims to emulate private-sector best practices (e.g., incite competition and improve cost efficiency). Thus, a private-sector definition of governance should suffice. Daily, Dalton, and Cannella, Jr. (2003) define corporate governance as "the determination of the broad uses to which organizational resources will be deployed and the resolution of conflicts among the myriad participants in organizations" (p. 371). Governance consists of the policies, rules, organization, and processes to properly manage program decision-making. This differs from management, which is concerned with the implementation of rules and processes. Governance is the framework within which managers operate. A proper SoS governance structure will allow the members of the organization—from program managers to engineers, scientists, and support staff—to effectively operate.

## *Platform-Centric Governance*

The DoD is organized hierarchically, as are most private-sector corporations, and the traditional, or platform-centric, program governance system is, likewise, hierarchical. Policies, regulations, and directives flow vertically, with few horizontal interactions. In both sectors, there is a clear chain of command. Within the DoD, the hierarchical structure is reproduced recursively at each level of command. Moreover, authority is often segmented with different Services overseeing projects within their respective domains (air, land, or sea). At lower levels, program managers oversee the acquisition of individual weapons and systems to include their development, testing, repair, and disposal (see Figure 1). Unfortunately, hierarchical structures are not well-suited to the SoS environment, which, in theory, takes the form of "a web of shared interests" rather than a hierarchical chain of command (Morris, Place, & Smith, 2006).

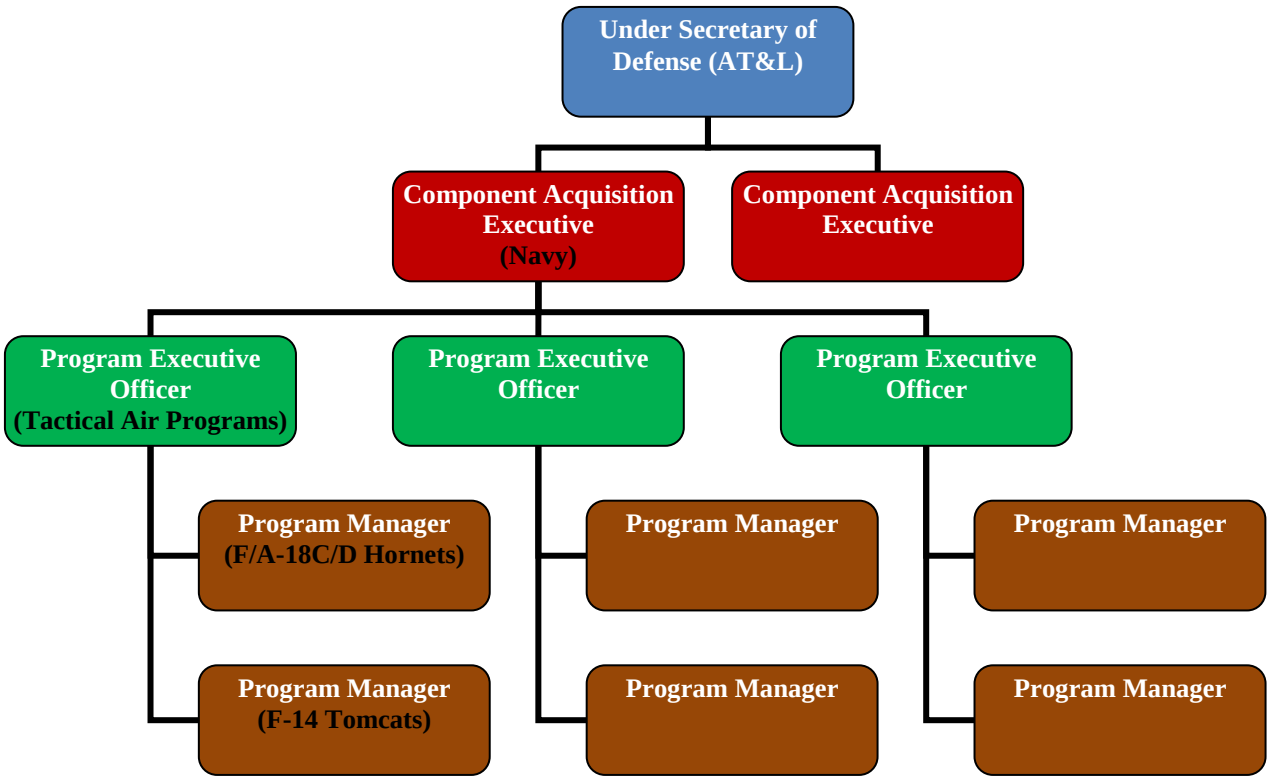


**Figure 1. Platform-Centric Governance**

Figure 1 is a simplified representation of the current governance structure. Rather than flowing horizontally, decisions and information flow vertically, from the Under Secretary of Defense for Acquisition, Technology, and Logistics to the various Service and agency component executives, to the program executive officers (PEOs). The PEOs oversee large programs or a portfolio of smaller ones, each of which is led by a program manager. Though this governance structure simplifies tasks, it fails to facilitate interoperability and SoS-level optimization. In fact, one could argue that the traditional hierarchical governance structure is poorly suited to the acquisition of individual platforms, too. SoS considerations aside, the traditional structure is inflexible, formalized, centralized, and rule intensive—all characteristics of the "classic machine bureaucracy" (Dillard, 2008, p. 259). Moreover, a program's actual governance structure is considerably more complex than the diagram above suggests. There are numerous interactions between various stakeholders at every level. A program's governance is impacted, directly or indirectly, by myriad groups—from Congress, to the Office of Management and Budget, to the GAO and DoD Inspector General, to appointees, test commands, staffers, and the users

themselves. Indeed, the input from these entities may prove vital to a program's success; however, the hierarchical structure, which has no mechanism to formalize intergroup collaboration, is often unable to translate valuable input into tangible program outputs. The structure is also less flexible than the diagram suggests. Often, for instance, program executive officers are unable to reallocate funding among the programs under their control because funds are appropriated by Congress to each individual program.

Cost overruns have been commonplace since the 1960s, despite numerous policies aimed at reforming the acquisition process (Jones, 2011). Platform-centric governance, it appears, has not proven to be an effective strategy, even in the pre-SoS environment. In any case, it is clear that attempting to develop even more capable systems-of-systems within the current structure will result in yet greater failure. Indeed, the "platform" as a construct, is being deemphasized by military leaders. Recently, retired General James Cartwright (former vice chairman of the Joint Chiefs of Staffs) noted, "Spending 20 years in development of a platform and then building it … all seems somewhat irrelevant" (Pincus, 2012, p. 1). Rather, swift upgrades and spin-outs within the context of constantly evolving technology will characterize future military acquisitions. In a similar vein, Colonel Ray Jones (2007) argues that a capability-centered acquisition strategy should be implemented. Under this strategy, there may be many material solutions, or conversely, a single material solution capable of performing the functions of multiple platforms. The objective is to determine the best-value solution among an array of possibilities (Jones, 2007).

Despite the rigidity of existing governance structures, program managers have successfully injected some flexibility into the system by, for example, organizing teams in ad hoc fashion to work on program-specific tasks that are not formalized within the standard governance structure. In fact, the DoD has implemented initiatives over the last couple of decades, such as integrated product teams (IPTs), to facilitate this tendency among managers. An IPT consists of a small group of cross-functional, multidisciplinary members, dedicated to a specific task (see Figure 2). Regrettably, this level of organizational integration does not often exist at the higher levels within the DoD's governance structure. As a result, the decision to, for example, modify one

system is often made in isolation, even though it will invariably have an impact on other systems within the DoD's inventory of systems.

As John Dillard (2008) points out, the IPT philosophy has also come to inform command and control tactics as well, with emphasis being placed on transmitting essential information to the "tactical edge." Both on and off the battlefield, the DoD has begun to recognize the advantage of empowering lower level personnel in order to "transfer knowledge and power to the point of an organization's interaction with its environment" (Dillard, 2008, p. 261). Research in organization theory (e.g., Engwall, 2003; Thomas & Buckle, 2004) supports the DoD's move to decentralize control via the empowerment of lower level entities.

However, decentralization is no panacea, especially with regard to SoS; in fact, it can be a considerable liability. Whereas a decentralized approach may work well when acquiring a typical system consisting of highly defined subsystems and components (e.g., aircraft), the same cannot be said for novel SoS with evolving requirements. Unfortunately, however, the human mind exhibits a preference for binary oppositions. If a highly centralized management approach fails to produce the desired results, then we assume that a highly decentralized approach must be the answer. In government, diametrically opposed policies and procedures come and go, as the pendulum swings from one extreme to the other. As it turns out, the best approach often consists of a mix; in the case of SoS governance, a structure wherein certain processes are centralized and others are not, may prove superior. Past SoS programs—three of which are described in the next section of this report— bear this out, as does emerging research. For instance, Ivory and Alderman (2005) assert that "local empowerment and intervention to correct errors, along with top-down responsiveness to embed learning across the systems … is critical" (p. 8).

### *Integrated Product Teams*

The *DoD Integrated Product and Process Development Handbook* defines an integrated product team (IPT) as "a multidisciplinary group of people who are collectively responsible for delivering a defined product or process" (OUSD[AT&L], 1996, ch. 10.3). According to the *Handbook*, the IPT is composed of people who plan, execute, and implement life-cycle decisions for the system being acquired. This group can include contractors, stakeholders, and other empowered representatives from all of the functional areas of the product, including those involved with the design, manufacturing, test and evaluation (T&E), and logistics personnel. The customer may also be included. The *Handbook* states that "because the activities relative to a system's acquisition change and evolve over its life cycle, the roles of various IPTs and IPT members evolve" (ch. 10.3). Moreover, "when the team is dealing with an area that requires a specific expertise, the role of the member with that expertise will predominate; however, other team members' input should be integrated into the overall life-cycle design of the product" (ch. 10.3). Some teams may assemble, often in ad hoc fashion, to address a specific problem and then become inactive or even disband after accomplishing the task in question. An example of a Program Management Office IPT structure used to acquire a military vehicle is provided in Figure 2.

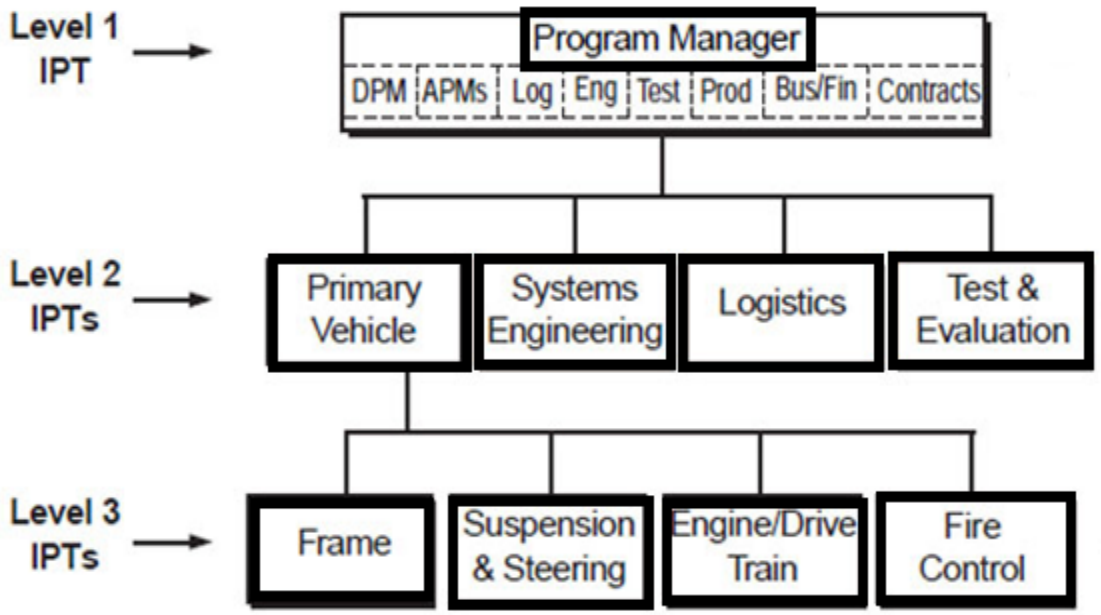


**Figure 2. Example of a Program Management Office IPT Structure**

(DAU, 2011)

## *SoS Governance*

In 1998, Maier described three categories of SoS from a governance perspective: directed, virtual, and collaborative. The *Defense Acquisition Guidebook* (*DAG*; DAU, 2011) recognizes a fourth category, "acknowledged." The *DAG* descriptions of these categories are provided in Table 2.

| | |
|---|---|
| **Virtual** | Virtual SoS lack a central management authority and a centrally agreed-upon purpose for the SoS. Large-scale behavior emerges—and may be desirable—but this type of SoS should rely upon relatively invisible mechanisms to maintain it. |
| **Collaborative** | In collaborative SoS, the component systems interact more or less voluntarily to fulfill agreed-upon central purposes. The Internet is a collaborative system. The Internet Engineering Task Force works out standards, but has no power to enforce them. The central players collectively decide how to provide or deny service, thereby providing some means of enforcing and maintaining standards. |
| **Acknowledged** | Acknowledged SoS have recognized objectives, a designated manager, and resources for the SoS; however, the constituent systems retain their independent ownership, objectives, funding, and development and sustainment approaches. Changes in the systems are based on collaboration between the SoS and the individual systems. |
| **Directed** | Directed SoS are those in which the integrated SoS is built and managed to fulfill specific purposes. It is centrally managed during long-term operation to continue to fulfill those purposes as well as any new ones the system owners might wish to address. The component systems maintain an ability to operate independently, but their normal operational mode is subordinated to the centrally managed purpose. |

**Table 2. Categories of Systems-of-Systems**
(DAU, 2011)

SoS governance requires collaboration and integration across programs and assets. Decisions and trade-offs need to be made at levels higher than the individual system. The distributed ownership of individual systems creates a problem that governance mechanisms must be designed to address. Without adequate mechanisms, individual system program managers will develop their systems in accordance with their localized priorities, which will compromise the efficiency and effectiveness of the SoS (Morris, Place, & Smith, 2006). Furthermore, any unforeseen challenges with regard to the technical implementation of certain systems/components can exacerbate this problem; indeed, such challenges often arise when owners of different systems assume that they are (or are not) responsible for implementing a specific element of the SoS, resulting in technical deficits or redundancies that can render elements of the SoS noninteroperable.

The above typology suggests that in some instances (e.g., "acknowledged" SoS, where constituent systems retain their independent ownership) a decentralized approach to acquisition may be appropriate. Add to this the finding in the literature, discussed previously, that decentralization via local empowerment is a proven acquisition approach, and it becomes easier to see why SoS programs may underestimate the importance of purposeful integration, which necessarily entails the presence of a central, higher level authority. Decentralizing an SoS program by delegating complete responsibility for the development of constituent systems to different entities is rarely appropriate. In such instances, those in charge, other stakeholders, and the end users can only "hope" that the system evolves in accordance with expectations (which may vary across groups). When constituent systems are developed in isolation by different entities, it should not be assumed that integration will occur, even if the SoS in question is under the management of a single program office or program executive office.

It is tempting to view each of these four categories as discrete entities requiring different governance structures. But in reality, all SoS integration must be "directed" to some degree. We contend that each category of SoS can be governed using similar mechanisms and that it is merely the extent to which these various governing mechanisms are applied that will vary. In fact, the nature of the individual program dictates the use of these mechanisms more so than their category assignment. To say, for example, that an SoS is "directed" and, therefore, subordinated to a "central managed purpose" does not imply that all of the technical interactions between

systems can be engineered—or even articulated—in advance. Rather, one of the fundamental goals of SoS governance is to map a trajectory along which the program in question can grow and evolve. In reality, there is no single best SoS governance structure. In fact, the most successful regimes are, to a great extent, self-organizing. The ideal structure will draw on a variety of governance mechanisms in order to facilitate a flexible strategic process (Miller & Hobbs, 2005). The structure may incorporate characteristics of different governance regimes, including markets, contracts, hierarchies, budgets, and associations (North, 1990; Miller & Hobbs, 2005).

Unfortunately, the will to develop new criteria and better processes is often lacking. That is, it is rather unusual for a program manager or other official to invite scrutiny of either the project itself or the processes that are in place for the development, selection, and governance of projects (Miller & Hobbs, 2005). This lack of political will, though undesirable, is less problematic under traditional governance regimes. The deficiencies of such a regime are often well known, with all actors aware of operating procedures. They know the shortcuts, and how to accomplish goals under the prevailing circumstances. However, in an SoS environment, the development of new, more efficient processes and the will to scrutinize— and be scrutinized—is essential (Miller & Hobbs, 2005). As mentioned earlier, when it comes to large projects, we tend to gravitate toward simple solutions based on simple constructs (e.g., centralized vs. decentralized), while compartmentalizing individual responsibilities, assuming that, like a puzzle, the pieces will come together in the end.

But, this way of thinking is unrealistic, especially with regard to SoS, where disruptions in the development of one system can have unanticipated consequences on the development of others (DeLaurentis & Mane, 2010). Psychiatrist W. Ross Ashby (1956) realized this some time ago. His Rule of Requisite Variety asserts, “The larger the variety of actions available to a control system, the larger the variety of perturbations it is able to compensate.” Extrapolating from this rule, an organization’s structure and governance strategy must be matched to its environment in order to achieve optimal performance (Dillard, 2008).

In the past, individual DoD programs responsible for the acquisition of constituent systems have formed alliances (sharing resources, skills, and competencies) with mixed results. In such situations, the constituent systems retained their independent ownership, as well as their own objectives, funding, development, and sustainment approaches. But as mentioned, virtually all of today's military SoS require, to some degree, the purposeful integration of platforms.

The challenge of SoS governance, then, is achieving a balance; directing growth via firm protocols so as to avoid functional redundancies and component optimization (as opposed to overall SoS optimization) without stifling the emergence of unanticipated (though desirable) linkages and emergent behaviors. This will require incisive decision-making. When SoS programs are unbalanced, problems occur. On the one hand, programs exhibiting an overreliance on open architectures[2] may suffer from a lack of upfront systems engineering. Program personnel may assume, incorrectly, that an open systems architecture, which is responsive by nature to changes in technology and is flexible in design to accommodate technological advances in software and hardware, may obviate the need for upfront engineering, planning, and deliberate integration. SoS are intended to have wide-ranging impact, from platforms to organizational structures, training, tactics, and doctrine. Thus, from a decision-making perspective, it is critical to understand how the different elements of the program will interact, in order to ensure the optimal level of integration and interoperability.

Needless to say, the sheer size, scope, and duration of SoS programs complicate this decision-making process. For instance, Sengupta, Abdel-Hamid, and Van Wassenhove (2008) conducted a series of experiments revealing that even experienced program managers are often unable to incorporate the effects of time lags (i.e., the length of time between a decision and its result) into their initial planning decisions; rather, they make decisions within the context of a simplified "mental model" where "there is little or no delay between a decision and its result" (p. 97). Because SoS programs have long durations—in each of the SoS examples we present in the next section, even the programs' "vision statements" change dramatically over time—failing to account for time lags is highly problematic.

[2] A system architecture is the conceptual model that defines the structure and/or behavior of a system. An open system architecture is vendor independent and non-proprietary.

As mentioned, military leaders must take into account the unique characteristics of each SoS program in establishing a governance structure. That said, certain elements of SoS governance can be discussed generically. For instance, all SoS programs must establish a management strategy, risk assessment techniques, oversight and responsibility functions, and interoperability requirements. From the theoretical perspective, these mechanisms of SoS governance should be similar, at least in some respects, across programs. For instance, proper management of an SoS requires that decision-makers have visibility over the entire range of constituent systems. Decisions made about individual components or systems will have ripple effects on the other elements within the system. Without visibility, and, of course, the authority to act, it is difficult to mitigate these effects. Given the size, scope, and duration of SoS programs, each management decision carries greater implications. Managers must be highly qualified and demonstrate a proven ability to operate in complex environments and to incorporate the effects of time lags and non-linear system interactions into their planning decisions.

In addition, the sheer size, scope, and level of technical complexity demand that program personnel prioritize risk assessment. Moreover, SoS development engenders a new set of risks that the governance structure must be designed to address. Some of these risks include

- overlooked or underutilized functionalities or interfaces;
- undesirable emergent behavior;
- constituent systems/components that evolve to the extent that they are no longer compliant with original standards; and
- evolution of SoS that deviates from stakeholder needs (Piaszczyk, 2011).

Accountability is also important. When different assets within an SoS fail to interoperate, it can be difficult to hold accountable the responsible party. This challenge is compounded when the SoS in question relies on collaboration across programs or Service branches. A lack of accountability often results in cost overruns, schedule delays, and poor performance, because leadership is unable to determine which individuals/teams perform well and which perform unsatisfactorily (Kerzner, 2004). A good SoS governance structure must emphasize accountability by clearly defining individual roles.

Finally, to ensure systems integration, modifications may have to be made after system testing. The governance structure must be capable of determining which element of the SoS should be modified, who is responsible to oversee the work, and, in a multiple program environment, which office's budget will cover the costs.

# IV. SoS Governance in Practice

In the past, individual programs responsible for the acquisition of constituent systems have shared resources, skills, and competencies in order to acquire the SoS. In these situations, the constituent systems retained their own objectives, funding, development, and sustainment approaches. In other cases, the acquiring agency has relied on private-sector contractors, and their subcontractors, to acquire the SoS in its entirety. In these cases, the contractor performed many of the functions normally associated with program governance. In this section, we examine SoS programs in both of these categories in order to determine how actual governance contrasts with the theoretical considerations that we put forth in the previous section. Ultimately, this analysis will be used to inform our recommendations on how to improve SoS governance going forward.

In the following sections, we examine three SoS acquisition programs: the Coast Guard's Integrated Deepwater System Project, the Joint Tactical Radio System, and the Army's Future Combat Systems. We begin each section with a short description of the program, followed by a discussion of the lessons learned from each program. Then, in Part V, we examine these lessons within the context of program governance.

## *Project Deepwater*

By the early 1990s, the U.S. Coast Guard (USCG) began to recognize that its fleet required modernization. The USCG decided that a targeted SoS approach that integrated assets would maximize the Service's capabilities. The USCG Deepwater program illustrates one of the largest SoS development projects to date. The project was originally estimated to cost $24.2 billion and was scheduled to be completed in 2027. Two different acquisition strategies have been employed. First, a contractor performed the role of lead systems integrator (LSI), managing most aspects of the acquisition. However, on account of its poor performance, USCG officially assumed the duties of the LSI in April 2007.

Interoperability was the driving force behind the USCG's modernization effort. A common rescue mission often required a coordinated strategy between helicopters, multiple ship classes,

planes, satellites, and a command and control center. The USCG recognized that they lacked the internal capabilities to design, develop, and source the various components of Deepwater. This resulted in the selection of a private-sector LSI, chosen from multiple bids, to lead the development project. A joint collaboration between Lockheed Martin and Northrop Grumman, named Integrated Coast Guard Systems (ICGS), was selected. ICGS was responsible for designing, constructing, deploying, supporting, and integrating the Deepwater system, which included new assets as well as modifications to legacy systems.

The contract was structured as a performance-based agreement that held the LSI accountable for its development decisions. In other words, the contractor was responsible for the delivery of defined capabilities—not just specific assets. According to the contract, the USCG would retain system-wide decision authority. However, the contract provided the LSI with the flexibility to determine the outputs. The USCG "has specified the outcomes it is seeking to achieve and has given the system integrator responsibility for identifying and delivering the assets needed to achieve these outcomes" (GAO, 2004). In contrast, a typical contract for an acquisition project stipulates strict technical requirements, including the specification of platforms, before program initiation. ICGS proposed that the USCG acquire five new sea vessels, two fixed-wing aircraft, two helicopters, two unmanned aerial vehicles, and new or updated command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) assets. ICGS also proposed that the USCG upgrade several existing assets (see Table 3).

In effect, the indefinite delivery-indefinite quantity (IDIQ)[3] contract allowed the USCG to purchase unspecified quantities of specified outputs (cutters, aircraft, command and control assets, and so forth). Although the IDIQ contract provided the Coast Guard with more flexibility to respond to issues as they arose, the contract also increased the unit cost of assets, because the LSI was unable to economically plan the procurement of materials and long lead items in advance.

[3] An indefinite delivery-indefinite quantity (IDIQ or ID/IQ) contract provides for an indefinite quantity with stated limits of supplies or services during a fixed period.

| Name of Asset | Description of Asset Capabilities |
|---|---|
| National Security Cutter | Extended on-scene presence, long transits, and forward deployment worldwide |
| Fast Response Cutter | Multi-mission patrol boat with high readiness, speed, adaptability, and endurance |
| Offshore Patrol Cutter | Long-distance transit, extended on-scene presence, operations with multiple aircraft and boats |
| Long-Range Interceptor | Deployable from FCS and OPC for vessel boarding, pursuit and interdiction, and search and rescue operations |
| Short-Range Prosecutor | Deployable from FCS and OPC for law enforcement operations and to perform search and rescue operations |
| HC-144A Maritime Patrol Aircraft | Transportation and surveillance |
| HC-130J Long-Range Surveillance Aircraft | Surveillance and information coordination |
| HH-65 Multimission Cutter Helicopter | Short-range recovery helicopter |
| HH-60 Medium-Range Recovery Helicopter | Medium-range recovery helicopter |
| High Altitude Endurance Unmanned Air Vehicle | Large area surveillance |
| Vertical Unmanned Aerial Vehicle | Cutter-based asset to provide extended surveillance |

**Table 3. Description of Deepwater Assets**
This table was created using information from the GAO (GAO, 2008a, 2008b).

ICGS encountered challenges throughout the development process. For example, one of the initial projects, conversion of the 110-foot cutters to 123 feet, experienced significant problems. After extending the cutters, engineers realized the hull had structural deficiencies that caused buckling. This required additional corrective modifications to strengthen the hull. Once these were completed, further inspections revealed additional structural inadequacies that were subsequently discovered in all of the ships scheduled to be converted. Accordingly, the conversion project was cancelled in June 2005. ICGS and USCG engineers came forward after the cancellation to testify that the issues were foreseeable and that both the USCG and ICGS purposefully ignored obvious warnings. Testimony from ICGS representatives countered these claims (Lipton, 2006).

In April 2007, the USCG relieved ICGS of LSI responsibilities, citing poor performance. As one article noted, "the need for new assets grows ever more urgent as costly repairs on legacy assets continue to eat away at the funds available for a recapitalized fleet" (Munns, 2007). The USCG has since assumed the systems-of-systems integration responsibilities. In addition, USCG has altered the management of the Deepwater project, including a "reorganized acquisition directorate, a shift to acquiring Deepwater assets individually as opposed to through an SoS approach, and efforts to improve information to analyze and evaluate progress" (Hutton & Caldwell, 2008). Despite the USCG's displeasure with the Lockheed Martin-Northrop Grumman team, it retained the partnership as the primary contractor and principal development partner. Given the USCG's lack of qualified personnel to staff all management positions—vacancy rates were as high as 20% in 2008— many private contractors continued to fill important vacancies within the Deepwater project through 2012. Partially on account of the Coast Guard's experience with ICGS, legislation has been crafted to restrict the use of contractor LSIs on government programs. In 2010, the DoD prohibited the use of contractor LSIs on new programs.

**Lessons Learned**

- The USCG underestimated the required funding. An audit by the Government Accountability Office (GAO) in 2010 found the original estimate of $24.2 billion underestimated the true cost, which it put at $28 billion. Given the size of the project, this shortfall of $3.8 billion is, perhaps, understandable. The price of materials needed to build each asset fluctuated as commodity prices changed. Relatively small changes in the prices of steel, oil, copper, and nickel resulted in large swings in estimates. However, in an environment consisting of multiple, tightly coupled, interdependent systems, minor perturbations in one system spread quickly, negatively impacting the development of other systems.

  Deepwater relied on yearly appropriations from Congress for funding. Imprecise price estimates, coupled with miscalculated bids—companies tend to underestimate cost in initial bids in order to win a contract— resulted in inadequate funding. The lack of funding resulted in significant delays, which increased costs further. In addition, budgetary trade-offs during development were rare, especially after the program's

reorganization because funds were designated to each asset, rather than to the system as a whole, encouraging the optimization of each asset. Indeed, no system came in under budget; rather, most required additional funding.

- Contracting for a lead systems integrator did not relieve the USCG of its oversight responsibilities. The USCG's ineffective oversight of the LSI's management contributed to major development problems. Without the necessary oversight, problems were not caught at an early stage of development. There were no interventions on the part of the USCG prior to the restructuring. The USCG failed to manage the contract properly for a number of reasons. First, critics have often cited "unfavorable contract terms and conditions, poorly defined performance requirements, and inadequate management and technical oversight … [in addition to] vague contract terms and conditions [as having] compromised the Coast Guard's ability to hold the contractor accountable" (*The United States*, 2007). Differing interpretations of managerial responsibilities and even key performance requirements have undermined accountability.

- An inadequate organic workforce precluded sufficient oversight. The Coast Guard did not have the necessary human capital and technical ability to manage or even oversee the management of a project as large and complex as Deepwater. The USCG was unable to staff all of the acquisition positions, even when the LSI was principally responsible for managing the development of Deepwater. In at least some instances, negligence was the cause of lapsed managerial oversight. For example, in the middle of November 2006, Congress discovered that "the Coast Guard withheld from Congress warnings raised more than two years [prior] by its chief engineer about structural design flaws in its new National Security Cutter" (Lipton, 2006, p. 1). Although the USCG was aware of concerns regarding the development of certain Deepwater assets, it did not seek clarification or modification at that point in time, leading to subsequent schedule slips and cost increases along with strained relations with Congress. Simply put, the apparent lack of accountability and diffuse responsibility created an environment where no one felt compelled to intervene, even as problems became apparent.

- The IPTs performed poorly. After the 2005 restructuring, the USCG and ICGS adopted the use of IPTs, which, as previously described, are composed of personnel from each area of an organization in order to centralize the expertise needed to design, develop, test, and manufacture a product. The intended goal of IPTs was to increase flexibility by reducing oversight to a manageable level and empowering teams. IPTs can be valuable to SoS development because they allow for the collaboration and flexibility necessary to maximize system-level capabilities. IPTs in the Deepwater program consisted of personnel from the USCG, Northrop Grumman, and Lockheed Martin. However, the Deepwater IPTs performed poorly. They lacked a clear charter and failed to outline group and individual authority, performance goals, resources, or schedules, which arguably, should have been supplied by a higher level, centralized program office. Team members lacked the necessary training and expertise to properly contribute. Additionally, high turnover and staffing difficulties prevented IPTs from being properly staffed. Finally, few IPTs were collocated, resulting in barriers to collaboration and communication.

- The failure to use specific language with regard to contracts and requirements proved disastrous. For instance, task orders for specific outputs "did not identify which party had decision-making authority over structural design specifications; the conditions under which third-party assessment of the design would be necessary, or which organizations would be qualified to perform this role" (Brown, Potoski, & Van Slyke, 2008, p. 33).

- During initial Deepwater development, there were no quantifiable metrics for performance. As a result, the USCG was awarding performance bonuses to ICGS (which was given an 87% overall rating), despite clear evidence that Deepwater was not proceeding as scheduled. Prior to Deepwater, the USCG's assets were not fully interoperable, having been developed and acquired over several years. Given the wider range of missions assigned to the modern Coast Guard, asset versatility and interoperability were deemed essential. But mandating interoperability is difficult if system requirements have yet to be determined. Of course, over the course of a 25-year contract, technology evolves and needs and missions change. But this does not mean that initial requirements can be vaguely articulated or postponed until things take shape. Yet,

according to the USCG, it "could not know exactly all that it wanted each asset to do until it deployed its first-in-class and experimented with it under various conditions" (Brown, Potoski, & Van Slyke, 2008, p. 31). This attitude, though seemingly rational, makes the purposeful integration of systems very difficult.

### *The Joint Tactical Radio System*

In 1997, the Department of Defense (DoD) launched the Joint Tactical Radio System (JTRS; pronounced "jitters"), a transformational communications network that will permit warfighters and support personnel to seamlessly transmit voice, picture, and video via a high-capacity, wireless network. Since the program's inception, however, DoD officials have consistently overestimated the ease with which various components of JTRS could be developed and implemented. This has resulted in a program that has experienced delays, unforeseen technical hurdles, and major cost overruns.

JTRS is a software-defined radio (SDR), although it is more like a computer than a traditional radio. Functions that are traditionally built into a radio's hardware are, instead, implemented through software. As a result, with the proper software, JTRS can emulate a variety of different physical radios, but also has the ability to download data and imagery. An open systems framework, known as the Software Communications Architecture (SCA), is key to the system's interoperability; it "tells designers how elements of hardware and software are to operate in harmony" (Brown, Stricklan, & Babich, 2006, p. 1), thus enabling users of different JTRS variants (airborne, maritime, ground, fixed, etc.) to load and run the same software applications.

Initially, a joint program office (JPO) was established and tasked with development of the SCA; development of the JTRS radios themselves was divided into five clusters, each of which was headed by one of the military Services. For instance, the Air Force was tasked with developing JTRS for Air Force and Navy fixed-wing aircraft and helicopters, while the Army oversaw development of handheld, man-portable, and other small JTRS variants (see Table 4). The perceived simplicity behind the open architecture concept guided DoD officials in establishing this initial, decentralized management structure and acquisition strategy.

| Cluster | Lead Service | Responsibilities |
|---|---|---|
| **1** | Army | • Develop JTRS for Marine and Army ground vehicles, Air Force Tactical Air Control Parties (TACPs), and Army helicopters.<br>• Develop Wideband Networking Waveform (WNW), a next-generation Internet protocol (IP) based waveform to facilitate ad hoc mobile networking. |
| **2** | U.S. Special Operations Command | • Develop JTRS capabilities for existing handheld AN/PRC-148 Multiband Inter/Intra Team Radio (MBITR) to create a JTRS Enhanced MBITR (JEM). |
| **3** | Navy | • Develop Multifunctional Information Distribution System (MIDS) terminals. |
| **4** | Air Force | • Develop JTRS for Air Force and Navy fixed-wing aircraft and helicopters. |
| **5** | Army | • Develop handheld, man-portable, and other small JTRS variants. |

**Table 4. The Clusters Acquisition Approach**

*Note.* The information in this table came from the Joint Program Executive Office, Joint Tactical Radio System (JPEO JTRS; 2011).

The rationale behind the Service-led clusters approach relied upon a number of assumptions: (1) A universal, open architecture would provide a solid foundation on which to develop and produce interoperable JTRS variants, and (2) other technologies needed to create the end products were ancillary, easily acquired, and adaptable. In other words, the DoD expected the SCA "to provide the services with sufficiently developed hardware and software prototypes that they [could] use to immediately procure JTRS products" (General Accounting Office [GAO], 1999, p. 8). However, the JTRS program's failure to define the specific limitations of the available technology, and, instead, rely heavily on the SCA—a "responsive" and "flexible" architecture—led to the belief that difficult technical problems could be addressed further downstream. Technical problems notwithstanding, the lack of a more effective joint management structure led to the program's inability to control costs (GAO, 2003).

As the focus of the JTRS program transitioned from radio replacement to transformational networked communications, technical requirements were modified. "Requirements creep," or the continual enhancement of the requirements of a project as the system is being developed, was a serious problem that has delayed JTRS since its inception. More waveforms were added to the JTRS repertoire; power consumption, size, and weight requirements of several JTRS variants increased dramatically. As a result, none of the Services had a firm understanding of what a finished JTRS product might look like.

In March 2005, Congress mandated the creation of a more unified structure, a joint program executive office (JPEO), to coordinate development of the "siloed" radio technologies (see Figure 3). Unlike the JPO, where program managers reported to their own service executives, the JPEO was a well-defined management hierarchy headed by a joint program executive officer. The JPEO was a significant improvement; it centralized JTRS operations, reduced the scope of the program, revised deadlines, and was able to acquire additional funding. In addition to the creation of radio-specific (as opposed to military Service-specific) programs, the JPEO implemented an incremental approach to product development, thus permitting operational experience to inform future product requirements. The JPEO separated variants and components into phases, permitting subsequent iterations to incorporate proven technologies or design successes. The JPEO also encouraged commercial development of transitional radios to bridge the gap between current communications capabilities and the full implementation of JTRS.

The restructured JTRS JPEO currently manages four Major Defense Acquisition Programs (MDAPs): the Handheld, Manpack, and Small Form Fit (HMS); the Airborne, Maritime, and Fixed Station (AMF); the Multifunctional Information Distribution System (MIDS); and the Network Enterprise Domain (NED). The HMS program includes all portable ground radio variants that are not mounted on vehicles. The AMF will overhaul the numerous communications systems currently used by the military on fixed and rotary wing aircraft, ground installations, and a wide range of warships and submarines. The MIDS JTRS program is working to transform the existing MIDS Low Volume Terminal (MIDS-LVT)—a jam-resistant, single-channel secure voice and data non-software-defined radio—into a four-channel JTRS version to be used in different types of aircraft, ships, and ground stations. Finally, the NED program develops the

waveforms and provides the common networking services solutions to the other programs. A fifth MDAP, the Ground Mobile Radio (GMR), was canceled in October 2011, following a sharp reduction in quantity that led to an increase in the per-unit cost of the radios (Brewin, 2011). The GMR was a four-channel radio that was to provide multimedia communications over independent channels to ground vehicle platforms. Prior to the cancellation of the GMR, the DoD estimated that it would spend over $23 billion over the coming years to procure some 194,000 JTRS radios (Harrison, 2010). It is unclear if these funds will be reallocated or reduced in light of the elimination of the GMR program.

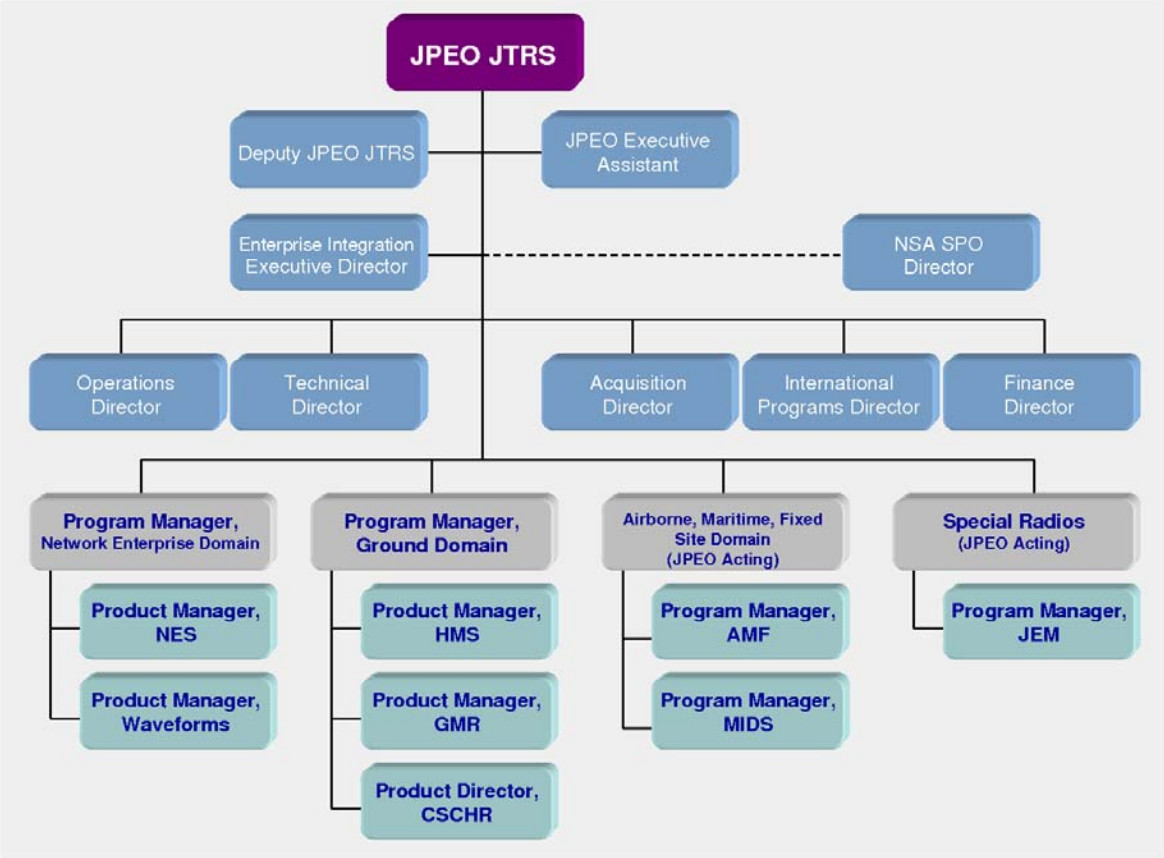


**Figure 3. JPEO Governance Structure**
(JPEO JTRS, 2011)

**Lessons Learned**

- The Service-centric approach proved inadequate. By dividing procurement responsibilities among the Services, all of the costs (research, development, fielding, etc.) associated with each radio variant were shouldered by the users of the end product. Though this strategy seemed the most equitable, it engendered a Service-centric approach, rather than a DoD-wide enterprise approach, and JTRS came to be viewed as a radio replacement program as opposed to a new, holistic enterprise-wide information infrastructure. The initial procurement of JTRS radios came to a halt in 2005 because of program cost overruns and insurmountable technical hurdles. Of the $856 million initial contract for Cluster 1 procurement, $573 million had been spent. Even after the reorganization, funding was allocated to individual systems through yearly congressional appropriations. The JPEO had little flexibility to reallocate costs as the program evolved.

- The evolution of JTRS deviated from stakeholder needs over time. It is important to remember that the DoD launched JTRS in 1997, long before the word "smartphone" was coined. In early 2012, the Army began experimenting with "marrying smartphones to handheld Riflemen Radios" that use the soldier radio waveform, allowing the smartphones to, in effect, "ride" on secure, established communications links without the need for cell phone towers (Magnuson, 2012, p. 1).

  Unfortunately, development of the algorithms for the JTRS waveforms began prior to the advent of mobile computing. According to Lewis Johnston, vice president of advanced programs for Thales Communications Inc., "the soldier radio waveform was not designed to handle all the processing power needed to run a smartphone" (Magnuson, 2012, p. 1). Running smartphone applications requires the use of the wideband networking waveform, which was not intended to run on handheld radios, but on base station and vehicle JTRS variants, which have larger batteries. Johnston noted that if the batteries can be made smaller, lighter, and more efficient or, conversely, the wideband networking waveform can be designed to use less battery power, the possibility of integrating smartphone technology with JTRS is a possibility (Magnuson, 2012).

Currently, some units are relying on private-sector companies to provide them with connectivity. For example, Lockheed Martin's MONAX system fits in two containers about the size of large trunks (Magnuson, 2012). The antenna provides a range of approximately 38 kilometers and can host more users than a typical commercial cellular tower (Magnuson, 2012). Harris Corp., and partner Battlefield Communications Systems, offers the NightHawk 3G, a cellular network designed for units that are on the move. It is currently being used in Afghanistan. And Twisted Pair, a Seattle-based company, has a tactical 4G command center cloud that, it asserts, allows all legacy radios and smartphones to interoperate. According to James Mustarde, director of marketing, "It allows secure communication between any device, between any user over any network. It's removing that tether that says, 'I'm a radio, therefore I have to speak to another guy on a radio'" (Magnuson, 2012, p. 1). Mustarde went on to say that "the device becomes almost irrelevant" and that "a person on a Cisco phone in the Pentagon can communicate with a soldier using a smartphone in the battlefield" (Magnuson, 2012, p. 1). He characterizes the current battlefield communications environment, stating, "You come to the table, you can eat off the table, as long as you have permission" (Magnuson, 2012, p. 1). Both the Army and U.S. Special Operations Command are Twisted Pair customers.

- The failure to oversee the concurrent development of waveforms and radios contributed significantly to the challenges and setbacks that the JTRS program has encountered since its inception. Program officials underestimated the complexity of the technology involved, leading them to believe that the SCA would be sufficient to adequately convey JTRS specifications to program personnel and government contractors. This assumption proved faulty, and contractors developed their systems based on their interpretations. Unforeseen challenges with regard to the technical implementation of certain components—and there were several—exacerbated this problem. Where were such challenges to be addressed—in the radio or in the waveform? The Network Enterprise Domain, responsible for waveform design, assumed that the radio contractors would address certain problems, and vice versa. This assumption was further aggravated by the pace of the program; if it takes 36–48 months to develop the hardware and/or software,

the open system standards have likely been updated several times. According to Colonel Ray Jones (personal communication, July 5, 2011), JTRS Deputy PEO, the majority of delays and cost increases within the enterprise were the direct result of unmet expectations on the part of the radio design contractors; in other words, the waveforms provided did not meet the design expectations of the contractors, each of which plugged unspecified technical gaps with unique hardware solutions or failed to address them altogether.

- There was no enterprise-wide systems engineering master plan. Accordingly, each radio was designed to meet Service-specific needs and desires with little regard for how the radio might fit within the overall network or integrate into different platforms. For instance, both Cluster 1 (led by the Army) and Cluster 4 (led by the Air Force) were tasked with the development of JTRS for their own helicopter platforms; Service-specific technical requirements, it appears, provided the rationale. Similarly, the JPO took on the responsibility for waveform development, but assigned the WNW, described previously, to Cluster 1. Moreover, there was no plan to formally test interoperability among the five clusters. To this day, inadequately defined interoperability goals continue to present a challenge to the JTRS program.

- The program undervalued the importance of purposeful integration of JTRS variants. In response to a GAO recommendation to delineate the limitations of commercial and DoD technology "in satisfying current and future JTRS requirements," the DoD asserted that "[JTRS'] open systems architecture is responsive by nature to changes in technology and is flexible in design to accommodate technological advances in software and hardware" (GAO, 1999, p. 29). Although this may be true in theory, there is some work that needs to be done to integrate specific applications. For instance, video from Unmanned Aerial Vehicles (UAVs) sent over Common Data Link (CDL) waveforms can be viewed currently only with the use of a Rover or Video Scout computer which, in turn, feeds the output into the JTRS radio via a plug-in device (Button, 2010). This means soldiers have to carry additional hardware, thereby defeating one of the very reasons for which JTRS was conceived, while adding significant operating costs.

Although the DoD had mandated that the CDL waveform be used for viewing video prior to the JTRS program's inception, it was not envisioned to be an initial JTRS required capability because it was outside the required frequency range. Currently, the DoD is funding research for the development of a "workaround" to add UAV video viewing capabilities to JTRS (Button, 2010, p. 1). A JTRS spokesman explained that the JPEO never considered adding the CDL waveforms to the JTRS repertoire because their use required excessive bandwidth (JTRS waveforms use frequencies between 2 megahertz and 2 gigahertz; the CDL is a higher frequency waveform, operating above 2 gigahertz). At the same time, the JTRS program had always planned to develop and acquire waveforms "above 2 GHz" at some point in the future (Baddeley, 2005).

- The lack of upfront systems engineering precluded an adequate assessment of platform integration. Often, the physical configuration and technical requirements of specific platforms were not adequately considered during the initial design phases; in some instances, it was unclear as to which platforms would even carry JTRS radios. Consider the case of the Bradley Fighting Vehicle whose Operational Requirements Document (ORD) specifies that all integrated systems must be rated up to 71 degrees Celsius (approximately 160 degrees Fahrenheit). The GMR, however, was designed to operate up to a maximum temperature of 55 degrees Celsius. In addition, the physical dimensions of the GMR were such that it could not be easily installed in the vehicles. In the end, it was decided that the GMR would not be installed in the Bradley. It appears that the platform given the most thorough consideration during the GMR design phase was the Manned Ground Vehicle, a component of the FCS program. Curiously, the FCS program, if realized, would have comprised only a fraction of the Army's combat brigades, the majority of which rely on the M1 Abrams tank and the Bradley. It is unclear why the configurations of these platforms were not given greater consideration.

- The program was out of touch with warfighters' needs. Vice Chief of Staff of the U.S. Army, Peter Chiarelli, for instance, notes how "struck" he was that JTRS engineers were worried about a 10-second latency in a certain JTRS radio (Erwin, 2010). He reasoned,

> "If I don't have that radio, troops have to go up a mountain to get line of sight and expose themselves to enemy fire. They'd much rather have a 10 second latency that allows them to remain concealed" (Erwin, 2010, p. 23).

### *Future Combat Systems*

The Army's Future Combat Systems (FCS) was the "Army's first full-spectrum modernization in nearly 40 years" (U.S. Army, 2007). The FCS originated as the combat portion of the Army's 2003 planned Future Force, the overarching strategy to prepare the Army for operation in the next century. The goal of this system was to "free ground warfare from the tyranny of terrain" (Scales, 2006). The Army believed that the new NCW doctrine would be critical to the development of a new agile and mobile force. The heart of the FCS SoS is an integrated information network that enables FCS assets to respond more rapidly to changing battlefield conditions and in a more coordinated manner than any opponent. In this way, the advanced information network is a force multiplier by providing military personal full battlespace awareness. Ultimately, the Army believed FCS would support NCW and offer the Service a force that is more responsive, more integrated, and more sustainable than its current force. However, the program was canceled in 2009 because of technical difficulties, major cost overruns, and the belief, at least among DoD leadership, that the program was poorly aligned with modern military objectives.

The Army determined that the army of the future, FCS, must embody two important changes. First, the Army needed to be much more deployable. Currently, deploying one of the Army's heavy brigades requires several months of planning and transportation. FCS was to be deployable within weeks or even days. Second, Army assets needed to remain light and maneuverable without sacrificing firepower to effectively counter both conventional and asymmetric threats. In order to accomplish this objective, FCS must be a system equipped as a light brigade with the capabilities of a heavy one. The FCS's ultimate goal was to "replace mass with superior information allowing soldiers to see and hit the enemy first, rather than to rely on heavy armor to withstand a hit" (GAO, 2007a). The FCS concept relies upon the use of superior technology and information to identify and engage the enemy at stand-off range before the

enemy can locate FCS assets. Accordingly, the Joint Tactical Radio System would be crucial to realizing these twin goals.

Each fielded FCS component, including the soldier, would act as a sensor on the battlefield. Information would be seamlessly transmitted across the network, both up and down the chain of command, to every other participant in the field, as well as to the command post. Together, this information would allow the Army to achieve the FCS's objective: "see first, understand first, act first, finish decisively" (Boeing Integrated Defense Systems, 2006, p.1).

In addition to achieving a decisive edge in combat, the Army believed that FCS would significantly reduce operational resources. Through purposeful intent, SoS development in FCS would increase the "tooth" of the force while minimizing the "tail." The Army hoped to achieve a "70-90% vehicle commonality [resulting in a] 60% reduction in mechanics,…50-70% reduction in force size and fuel consumption [and] … be 60 percent more strategically deployable than Current Forces" (Boeing Integrated Defense Systems, 2006, p.1). Each FCS brigade would require fewer troops than existing units while providing more combat soldiers, and require fewer resources to operate while being more easily deployable.

FCS was originally planned to field a system of 18 different weapons platforms, the soldier, and an information network. Congress initially funded only 14 of these weapons systems, however. The Army has dubbed this configuration "14+1+1": 14 weapons platforms, plus the advanced information network, plus the soldier. The 14 platforms included eight manned ground vehicles, two unmanned ground vehicles, two unmanned air vehicles, the non-line-of-sight launch system, and unattended ground sensors (see Figure 4).

The need to replace aging legacy weapons designed for the Cold War, combined with the need to fill gaps for units currently serving in conflicts in the Near East, prompted the Army to put forth an aggressive timetable for FCS development and acquisition. Program initiation in 2003 would be followed by the preliminary design review in 2009. Low-rate initial production was to commence in 2011, followed by a production decision in 2013. The first FCS brigade would have been equipped in 2015, followed by full-rate production in 2017. By 2030, the Army planned to have 15 FCS brigades.

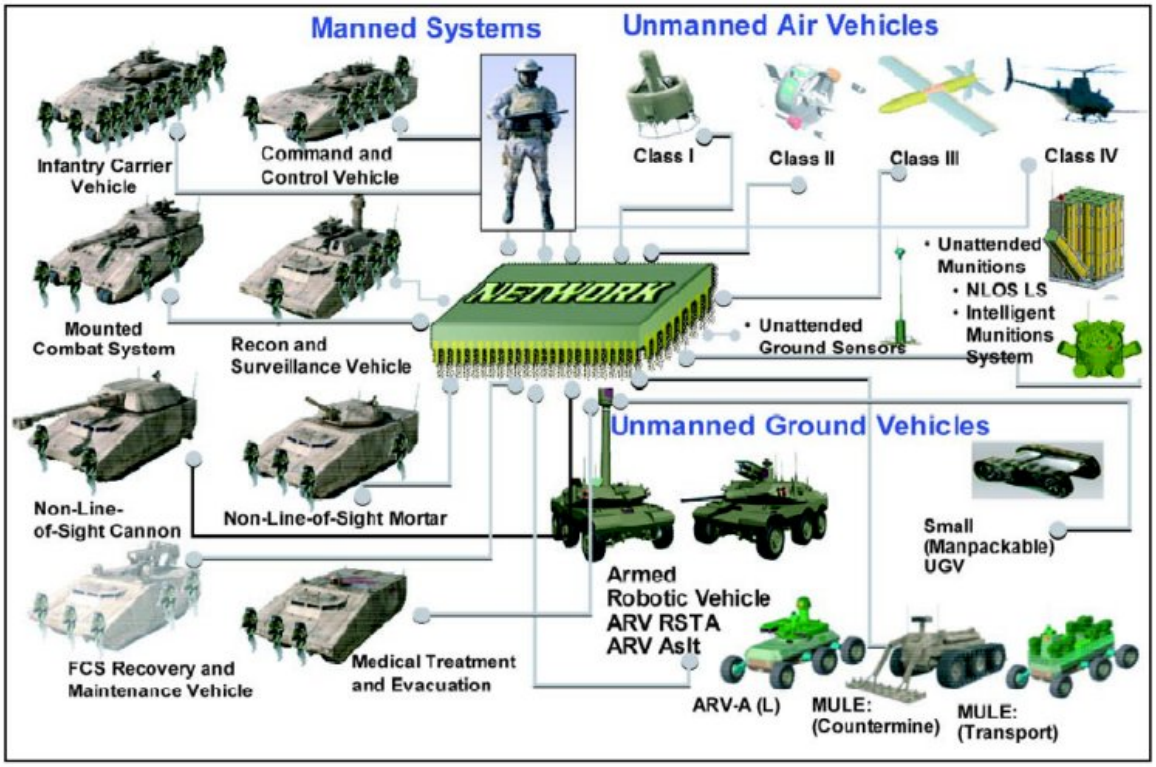


**Figure 4. FCS Assets**
("FCS Rolls On," 2005)

In November 1999, the Army teamed with the Defense Advanced Research Projects Agency (DARPA) to develop what would become the FCS concept. The Army and DARPA selected four contractor teams for an initial 21-month conceptual design phase, each worth $10 million. The four teams were Boeing Company Phantom Works; Science Applications International Corporation (SAIC); TEAM FoCuS Vision CONSORTIUM, a joint venture between General Dynamics Land Systems, Inc. and Raytheon Company; and Team Gladiator, a joint venture between TRW Incorporated, Lockheed Martin Incorporated, Lockheed Martin Vought Systems, CSC/Nichols Research, Carnegie Mellon Research Institute, Battelle Memorial Institute, and IITRI/AB Tech Group. During the bid process, in January 2002, two of the FCS bidders, Boeing and SAIC, decided to team and issue a joint bid. In March 2002, the Army awarded this partnership an LSI contract for the FCS' concept and technology development phase. The LSI was expected to make a $154 million profit for the 16-month effort (DoD & DARPA, 2002). DARPA and the Army originally planned to evaluate, in April 2003, whether technologies were mature enough to proceed with further development. The Army specifically granted the prime contractor, Boeing, SoS integration responsibilities because it did not believe it had "the

workforce or flexibility to manage development of FCS on its own within desired timelines" (GAO, 2007b). The Army believed that it lacked critical expertise and capability in key areas. For example, the Army did not believe it had enough software engineers to develop the information network; the managerial flexibility to respond to changing circumstances; the ability to effectively coordinate effort across the traditional organizational lines of the DoD, required for full network integration of the military; or enough capability to staff and manage a program as large and complex as FCS (GAO, 2007b). Under the traditional acquisition system, each of the 14 individual weapons systems along with the network would have been considered a major defense acquisition program, each requiring individual management, funding, IPTs, and so forth. Under FCS, the contracted LSI would provide consistent and continuous definition of requirements, development of technology, source selection, administrative coordination, and management of the allotted budget. Because the LSI would play such a large role in the acquisition of FCS, the entire program was placed under the authority of one program executive office, which was responsible for overseeing the LSI.

The Army put forth a demanding timetable for FCS development because it believed that the new challenges faced by the military must be met as quickly as possible. On account of the aggressive development timetable, the government would have insufficient time to reconstitute its own acquisition workforce. FCS could only be realized by partnering with a private firm to help oversee and manage development. After the events of 9/11, the Army began to develop the program immediately. In May 2003, it selected the Boeing-SAIC concept to proceed into the system development and demonstration phase (Boeing Integrated Defense Systems, 2003).

The Army and Boeing eventually signed an agreement for the systems design and development (SDD) phase in December 2003. To provide the program with greater flexibility, the Army opted for a non-standard instrument known as an Other Transaction Agreement[4] (OTA), which is not subject to the Federal Acquisition Regulation (FAR). Congress intended OTA, established in 1994, to be used for research, development, and prototyping with small innovative, commercial companies that were not part of the defense industrial base. Many of these small companies were

[4] An OTA is a special vehicle used by federal agencies for obtaining or advancing research and development (R&D) or prototypes. An OTA is not a contract, grant, or cooperative agreement, and it has no statutory or regulatory definition (Halchin, 2011).

previously excluded from competing for DoD contracts as they did not have the infrastructure to abide by the onerous reporting requirements of the FAR. The initial contract was for the first increment of the $91.4 billion, 17-year project (Francis, 2006). The agreement was a cost-reimbursement agreement for the first $14.8 billion development. This agreement included a "10% fixed fee, plus up to 5% in incentive awards – [for] a total of $2.2 billion in potential profit" (Cook, 2005).

The LSI was originally contracted to direct and manage the entire development process. The Boeing Company would also end up with responsibility for two important software-intensive subsystems: the System of Systems Common Operating Environment (SOSCOE) and the Warfighter Machine Interface (WMI). The SOSCOE is described as the operating system of FCS. This system is being developed by the LSI, which the OTA agreement permitted to "internally develop SOSCOE rather than contracting that work out to a separate supplier" (GAO, 2007b). The WMI is to provide an "integrated presentation of all types of battlefield information" (GAO, 2007b). Through competitive subcontracting, the LSI awarded the WMI to a separate Boeing operational unit.

FCS faced significant development difficulties exacerbated by federally mandated changes to the system. As a result, the program was reorganized twice. The first restructuring took place in July 2004 and expanded the scope of FCS by fully funding all 18 platforms originally envisioned by the FCS concept. This restructuring also created a spiral development framework that included four distinct spirals to field new technology to troops faster. The Army reorganized the program for two reasons. First, following 9/11, Congress increased funding for DoD development programs that allowed programs, such as FCS, to pursue more ambitious capabilities (Boeing Integrated Defense Systems, 2004). Second, the Army and Congress desired incremental fielding of assets to respond to challenges troops faced in the ongoing conflicts in Afghanistan and Iraq. The program adopted a spiral development acquisition strategy; as a result, assets would be fielded to troops more quickly, with the first increment planned to deploy in 2008. Proponents of this strategy also believed it would enhance the program's flexibility, enabling the developer to avoid technological bottlenecks that hampered other programs. However, the GAO warned in 2005 that the "program's level of knowledge is far below that suggested by best practices or

DoD policy: Nearly 2 years after program launch and with $4.6 billion invested, requirements are not firm and only 1 of over 50 technologies is mature" (GAO, 2005).

During 2005, the structure of the FCS contract was also changed. Under pressure from Senator John McCain (R-AZ), the Army agreed in April to restructure the OTA to a FAR-based contract. The new contract instituted an Organizational Conflict of Interest (OCI) provision to mitigate the LSIs' potential conflicts of interest. The provision has two important impacts. First, the LSIs are "prohibited from competing for work under the SDD contract at any tier" (Toenjes, 2008). Second, contractors are prohibited from participating in source selection "if any part of its organization submits a proposal" (Toenjes, 2008). Subcontracting agreements made prior to the restructuring of the contract remain in effect. The goal of these provisions is to eliminate the potential conflict of interest that would arise for a large company, such as Boeing or SAIC, to circumvent competitive subcontracting by awarding other divisions of the parent company contracts to develop a platform.

In 2006, the Army issued new cost and schedule estimates once it became apparent that the first restructuring would run significantly over budget and under schedule. The new estimate increased the total cost of the program from $91.4 billion to $160.7 billion, a 76% cost increase, while the program extended from 2020 to 2026 (Child, 2005). The increase in cost was attributed to the increase in the scope of the project and numerous technical development problems.

A second restructuring took place in early 2007. The principal goal of this restructuring was to maintain program costs within the new funding levels established in 2006. This restructuring both reduced the scope of FCS and reorganized programs within FCS. Program costs increased as a result of adding additional spin-outs of capabilities to current forces, extending the development rate, and including the previously unrecognized ammunition costs for FCS. Costs were reduced by deleting or deferring four systems, specifically the Class II and III unmanned aerial vehicles, the intelligent munitions system, and the armed robotic vehicle; changing (often reducing) the number of individual system assets to be purchased; and reducing the production rate for assets. The Army stated that costs were maintained (since the second restructuring),

while some outside sources cited substantially higher estimates (and, certainly, it was not a one-to-one comparison—given the quantity and scope changes).

In early 2009, it became clear that congressional support for FCS was waning. In February of that year, the Center for Strategic and International Studies wrote, "the Army will have spent 6 years and $18 billion on a system of interconnected weapon systems and warfighting software that are still largely developmental." In June 2009, Undersecretary of Defense Ashton Carter officially ended the FCS program. Replacing FCS is the Army Brigade Combat Team Modernization, which will bring together some FCS components under a "modernization plan" consisting of "separate but integrated" acquisition programs (Grant, 2009). These include efforts to provide technological upgrades, or spin outs to existing systems in the near term (Grant, 2009).

**Lessons Learned**

- The FCS budget was unstable from the program's inception. Over the first four years of development, the Army estimated that the total program costs would increase from $91.4 billion to $160.9 billion. Independent estimates produced in 2006, however, were considerably higher, citing figures between $203.3 billion and $233.9 billion. Though the LSI had authority to allocate and divert funding as it saw fit, there is some indication that it did not use funds as efficiently or effectively as possible.

- The DoD had final responsibility for all important decisions regarding FCS, but has been criticized for not exercising effective oversight of the LSI. Critics charged that lapses in oversight occurred because the government had no incentive, or was unwilling, to criticize its private-sector partners.

- The original, high fixed fee that scaled with increases in the price of the contract proved problematic, especially given the lack of DoD oversight. When the initial cost grew by $6.4 billion, Boeing received 15%, or approximately $960 million more in potential profits (Cook, 2005). Congress believed that this contract did not provide sufficient

incentive for Boeing to keep development costs low, as an increase in the price of the program would actually increase the overall profits of the company, all at the expense of the taxpayer. Because the DoD lacked the means to ensure that Boeing was, for example, selecting its subcontractors with the interests of the government in mind, Congress demanded that the Army and Boeing sign a new FAR-based contract in 2007, with a fixed fee of 3% and an incentive award of up to 12%. Congress also demanded that the conflict-of-interest issues regarding subsystems selections be properly addressed.

- FCS did not follow a knowledge-based acquisition strategy at program initiation; as a result, the program faced cost overruns, schedule delays, and reduction in capabilities. Technology risks were unacceptably high because certain subsystems were not tested on prototypes before production decisions were made. As mentioned, a problem in one component or constituent system can lead to major new cost, schedule, and performance problems across the entire program.

- The envisioned FCS capabilities began to deviate from warfighters' needs, despite program restructurings and requirements changes. The wars in Iraq and Afghanistan presented the Army with a need for new, unanticipated capabilities that, even when fully fielded, FCS would be unable to provide. For example, the unrelenting threat of improvised explosive devices (IEDs) increased demand for heavily armored vehicles. In response, the DoD authorized the rapid development and production of the Mine-Resistant-Ambush-Protected Vehicle (MRAP). In the late 1990s, military planners believed the increasingly mobile forces would be the key to future success. Yet, as casualty numbers rose and insurgents quickly shifted tactics, the solutions that better shielded soldiers—from upgrading armor to ultimately procuring MRAPs—began to replace earlier thinking. After the initial 1,185 MRAPs were fielded, the requirement for a total of 6,738 vehicles was approved in February 2007, increased again to 7,774 in May, and then to 15,374 by September (Brogan, 2007). The Services adjusted their demand for MRAP vehicles upwards and downwards in response to changing field conditions. By October 2009, requirements stood at 22,882. Although production of the MRAP represented the largest and fastest industrial mobilization since World War II,

nearly two years (20 months) passed from the time of the first formal field request for MRAPs, until validated requirements were obtained. Many critics of the procurement effort point to this long lag in the requirements process as a major failure. Former Marine Science and Technology Advisor Franz Gayl, who gained notoriety as a whistleblower on MRAP requirement delays, insisted that the 2005 Marine Urgent Universal Need request was intentionally ignored because MRAPs would divert funding away from existing development programs, including the Army's largest, the FCS.

# V. SoS Governance Challenges

There are a number of challenges to successful SoS governance. These challenges fall into five categories: leadership, management, requirements, human capital, and funding. We describe these challenges in this section.

## *Leadership*

- **Frequent leadership changes lead to program setbacks.**

  In theory, an SoS development is never complete. In practice, complex SoS programs may not begin to field useful capabilities for several years. Thus, political appointees in senior DoD leadership positions, serving an average of 18–24 months (Aerospace Industries Association, 2007), may have limited sustained impact on a program. In fact, political appointees may be less inclined to launch SoS programs in the first place, or fail to recommend an appropriate SoS governance structure, preferring instead to rely on a platform-centric approach that yields limited results more quickly.

  In addition, career government executives sometimes adopt a wait-and-see attitude with regard to incoming appointees. Executives, who "personify the cultures of their departments" and have "intimate knowledge on how things really are accomplished in day-to-day operations," may regard appointees' visions of their program as unrealistic (Parchem & Gowing, 2009, p. 1). According to Parchem and Gowing (2009) the collision of idealism and practicality "can cause the actual productivity of the organization to come to an abrupt halt" (p. 1).

  Frequent changes in senior leadership can also lead to significant changes in an organization's priorities, goals, and strategy. These changes can also significantly impact relationships with partnering organizations. At the program level, the lack of sustained leadership often contributes to program delays and setbacks, which can create tension among stakeholders. Frequent leadership turnover can also insulate and

strengthen the existing organizational culture. Long-term or permanent employees may be reluctant to participate in organizational change initiatives that significantly change their day-to-day responsibilities when the leaders who initiated these changes are not present to see them through, a potentiality that is more probable in the SoS environment.

- **Ineffective intergroup leadership inhibits collaboration.**

  Program personnel are, understandably, dedicated to their specific program office as well as its leadership. When personnel are also assigned to cross-functional teams composed of individuals from different programs—and possibly from different military Services and agencies—they may not recognize the importance of achieving successful outcomes, even if (perhaps especially if) the task involves the integration of different programs' systems. The desire to define oneself according to one's "home" group has been well-documented by leadership and organizational theorists (Abrams & Hogg, 2010). One consequence of this desire is that groups "strive to be separate from and superior to relevant out groups" (Hogg, van Knippenberg, & Rast, 2012, p. 236). In this sort of environment, it is no wonder that SoS programs, which rely on the collaborative effort of multiple groups, often fail to meet their assigned objectives.

  Hogg, van Knippenberg, and Rast (2012) attribute this to leadership's inability to foster an "intergroup relational identity," which they define as "self-definition in terms of one's group membership that incorporates the group's relationship with another group as part of the group's identity" (p. 233). Moreover, the notion often impressed upon members of a cross-functional team by its leadership, that their home groups are similar to one another, and, thus, possess similar objectives, merely reinforces feelings of separateness and superiority.

- **SoS vision statements change over time.**

  In all three of the examples provided in Part IV, the programs' vision statements changed radically over time. This is attributable to frequent leadership changes, but also

to rapid improvements in technology (especially within the commercial sector), and a changing battlefield environment. As a result, initial objectives and, thus, requirements are revised. Additional time and funding are required to develop new objectives. In the meantime, no new capabilities are fielded.

### *Management*

- **Managers of individual programs are not incentivized to ensure system-wide integration.**

  The system of checks and balances that is built into current governance structures often gives voice to existing organizational and cultural inertia and biases. Individual stakeholders—from contractors and Services' representatives to program managers, functional experts, and testers, often have objectives that are not completely aligned with those of the overall program, the focus of which is on the successful acquisition and delivery of an SoS. A good program manager works to develop system capabilities as cost effectively as possible, but because funding is appropriated to individual systems that are under the authority of different offices, there is often no incentive on the part of individual program offices to integrate these capabilities with those of other systems, particularly when integration costs are high, but the benefit is less obvious at the program level.

- **Management does not reward local interventions.**

  Project personnel working closely on a particular facet of a program rarely intervene to prevent potential system problems. In fact, intervention is often regarded as symptomatic of an earlier failure to properly plan and execute the project. However, in the SoS environment, where linkages and some emergent behaviors may be undesirable, personnel at all levels must be empowered to intervene as soon as a problem is detected.

## *Requirements*

- **SoS requirements are often overly ambitious.**

  Program decisions to begin design and/or production are made without sufficient knowledge. As a result, requirements tend to be overly ambitious, and, thus, unachievable. The DoD has two choices: improve knowledge or lower expectations. Because an SoS should not be designed as a final solution, but as an initial response to a problem (Keating et al., 2003), the latter is more appropriate. Users often subscribe to the notion that "more is better." Requirements are added that increase system complexity, which, in turn, calls for extending schedules—and budgets.

- **SoS requirements are constantly modified.**

  Requirements modification is especially problematic within the SoS environment. Adding, cancelling, or changing requirements has an impact on other constituent systems. More problematic still is that the precise nature of the impact often cannot be anticipated (from a technical, schedule, or cost point-of-view). At best, the owners of each system attempt to compensate for or otherwise facilitate the modifications to other systems as they occur. Of course, each time a modification is made, thorough simulation and testing is required. At worst, the requirements change goes unacknowledged, leading to serious interoperability challenges later on.

  The problem is two-fold. On the one hand, the process by which requirements are generated and approved is often ineffective. On the other hand, program governance structures often have no mechanism for validating or adjudicating interoperability requirements in the first place. Modifying requirements throughout development compounds the problem. As a result, long-duration SoS programs are viewed as works in progress that, ultimately, fail to deliver the initially envisioned functionality.

- **Platform design is not given adequate consideration.**

  In the SoS environment, the DoD's focus is on capabilities and objectives, often to the exclusion of platform design and integration. As mentioned previously, organizations have deemphasized the platform as a construct in favor of adopting an SoS approach, in some cases going too far. In some instances, it seems, capabilities are conceptualized in the abstract, untethered from the equipment upon which they rely. For example, the Coast Guard never adequately described the specifications of its desired fleet in concrete terms; rather, it determined the number of each asset and how it would contribute to the objectives set forth by the Coast Guard was the contractor's responsibility. Thus, it was virtually impossible for the Coast Guard to accurately assign costs to the program. Moreover, the contractor's interpretation of the objectives, and the requirements that needed to be designed to meet them, left the Coast Guard vulnerable to overpaying, and, ultimately, not receiving the capabilities it had anticipated.

## *Human Capital*

- **The DoD's workforce does not have the capacity to oversee complex SoS programs.**

  Currently, the DoD does not have the technical or managerial capability to oversee private-sector providers. In two of the programs we reviewed, organizations selected private firms to act as LSIs in an effort to overcome these shortfalls. But even in these instances, the government lacked the knowledgeable manpower necessary to ensure that the requirements were being met.

  Although it may make sense for the government to contract for technical augmentation (with the appropriate organizational conflict-of-interest safeguards), the DoD cannot outsource program management, as well as management and oversight of systems engineering, and expect to acquire efficient, affordable systems (National Research Council, 2008). Unfortunately, recruiting qualified, experienced systems engineers is a challenge, and not only for the DoD, but for industry, too. The production of systems

engineers by U.S. universities has increased, albeit very slowly over the past decade, despite a marked increase in demand, growing salaries, and other incentives.

- **Retaining high-quality managers is challenging.**

  As mentioned previously, hiring and retaining skilled personnel who have experience managing complex programs is essential to the success of the DoD's SoS programs. It is often assumed that highly qualified individuals tend to gravitate toward the private sector because the compensation is higher. This is partly true. A 2012 comparison by the CBO found that among workers whose education culminated in a bachelor's degree, the cost of total compensation averaged 15% more for federal workers than for similar workers in the private sector. Similarly, for those workers with a high school diploma or less, total compensation was about 36% more for federal employees. Conversely, total compensation for those with a professional degree or doctorate was 18% lower for federal employees compared to their private-sector counterparts.

  Accordingly, if the DoD seeks more highly educated managers, it must be prepared to pay them more. However, increasing compensation may not suffice. Highly skilled managers with proven abilities are attracted to the private sector for a variety of other reasons. For instance, the salary structure is less rigid, with proven ability figuring more prominently into how much one will be paid. In addition, there is the perception that the private sector allows for greater mobility.

## *Funding*

- **Funding is appropriated to individual systems.**

  In general, there is no single funding source for systems-of-systems. Rather, funding is programmed through the individual Services or through individual program offices for the individual system. As a result, there is no advocate for joint or, as the case may be, enterprise-wide capabilities. As a result, contracts are generally written that do not

adequately specify how the individual products are going to be integrated and tested with other elements into the SoS.

- **Funding is inflexible.**

  Even in instances when a central authority is tasked with allocating funds among different systems, funding is rarely reallocated in response to changes brought on by the SoS program's evolution. Once the funding is allocated, individual program offices intend to use it, and often go to considerable lengths to justify their expenses in the event that their funding levels are jeopardized.

# VI. The Way Forward

Given the current and anticipated budgetary environment and the increased political pressure to reduce defense spending, the DoD must improve the efficiency with which it develops, acquires, and fields complex systems-of-systems. However, given the number of organizational permutations that are possible, it is impractical to develop a single governance model. However, based on our theoretical discussion of systems-of-systems, the literature on the governance of complex projects, and our examination of past SoS programs, we can outline a notional governance structure, its attributes, and its composition.

A basic structure should consist of two levels. The lower level would be composed of officials representing the individual program offices, along with user representatives and other appropriate stakeholders. As one might expect, many SoS program-level functions (e.g., systems engineering, logistics, and test and evaluation) must also be performed at the level of the SoS to ensure the appropriate level of integration. This group would be tasked with coordinating these functions. In addition, this group, which we will term the Integration Working Group, must propose solutions for the problems identified across systems as they arise. These are then implemented by the appropriate program office. In the event that the issue cannot be resolved, or if consensus is not obtained, the problem is elevated to the upper level for adjudication. We will call this upper level the Senior Leadership Board.

The Senior Leadership Board would be led by the program executive officer, who is responsible and accountable for delivering the envisioned capabilities of the SoS. The other members of the Senior Leadership Board include program managers of the constituent systems, senior user representatives, and other appropriate stakeholders. In addition to resolving these issues, the Board would be responsible for maintaining the requirements baseline—restraining the natural tendency to make the programs "better." As the SoS evolves, and requirements change, ensuring systems integration becomes critical. The Board would be tasked with deciding which element(s) of the SoS should be modified, and how those changes are to be resourced.

Undoubtedly, this Senior Leadership Board, and or the Integration Working Group, will require an independent, system engineering firm to assist them in these technical trade-offs and oversight functions.

The governance structure must be designed to accommodate the unique features of the specific SoS program. Although there is no one-size-fits-all structure, a regime's design cannot be arbitrary, fluid, or nebulous. To the contrary, certain governance criteria (e.g., leadership, program management, the delegation of authority, requirements definition, risk assessment, oversight, integration, and funding) must be solidified prior to program initiation.

## *Recommendations*

Admittedly, SoS development and integration is complex and more abstract, which perhaps encourages program leadership to focus on the more intangible program elements (i.e., overall SoS capabilities, as opposed to platforms; objectives as opposed to requirements; and interoperability as opposed to physical integration) to the possible detriment of some program elements. Program leadership must walk a fine line; it must provide a conception of the SoS that is visionary, yet practical. We believe that the following recommendations, once implemented, will help leadership to achieve the correct balance.

- **Provide stable leadership.**

  Because of the added interdependencies and complexities of systems-of-systems, their successful development is even more dependent on continuity of leadership. Frequent changes in key personnel often mean changes in approaches to the overall effort, as well as the many supporting programs; these changes cause delays and impede the program's progress. To the degree possible, program continuity should be ensured, especially with regard to key senior leadership.

  Political appointees can be especially critical for high-profile systems-of-systems. To have a lasting impact on SoS programs during their short tenure, they must assume their role quickly by building relationships and networks with key stakeholders both

inside and outside of the organization and, perhaps most important, making an effort to understand the rules and beliefs held by key people in the organization (Parchem & Gowing, 2009).

- **Develop intergroup leadership and collaboration.**

  The governance structure must be aligned with the fielding of a functional, interoperable SoS that delivers the envisioned capabilities. However, it is often the case that personnel are focused on meeting the expectations of the organizations (e.g., program offices) that they represent, and not those of a governing body (e.g., the Integration Working Group) with little perceived power. Senior leaders must continuously emphasize to members of the Integration Working Group that collaboration is essential to achieving outcomes that are deeply valued by their respective organizations (Hogg, van Knippenburg, & Rast, 2012). Kelman (2012) asserts that leadership should also promote the idea that organizations' joint activities are capable of producing better results than the each organization could on its own. Management should also incentivize personnel at the program level to intervene in order to correct system deficiencies before they disrupt other systems. Program test personnel, for instance, must be incentivized to not only uncover the deficiencies or the technical oversights within a program, but should articulate how such problems might affect the SoS as a whole.

- **Ensure requirements stability by using an evolutionary approach.**

  SoS programs are dynamic, not static. Rapidly occurring external events and changing conditions are to be expected. However, initial requirements should remain fixed in the short term. The first increment of an SoS program must be designed, produced, and fielded so as to offer useful capabilities to the warfighter in as timely a manner as possible. Users' feedback and new capabilities should then be incorporated into future increments, which will help ensure that the SoS remains relevant over the long term.

  Unfortunately, it appears that within the DoD, there is a strong aversion to partial solutions. In the case of JTRS, for example, capabilities were not assigned to specific

increments; rather, they were frontloaded onto the initial requirements document. By adopting an evolutionary approach, the SoS Senior Leadership Board can maintain the requirements baseline without sacrificing the long-term SoS vision, for which it is also responsible. Under an evolutionary approach, essential technologies can be fielded in the near term, delaying the instantiation of more time-intensive, costly, or technically challenging capabilities.

An evolutionary approach helps to ensure the rapid deployment of systems, allowing program leadership to claim "early wins," which can be essential to maintaining congressional support over the long duration of the SoS program. When systems are developed incrementally, based on mature technology, the program risk is minimized.

- **Verify SoS integration.**

  Neither JTRS, nor the Deepwater program, determined how elements within the SoS would be integrated prior to production. In the case of Deepwater, the program decided to organize future systems and their requirements around the first systems to be deployed. Ideally, the Integration Working Group would assign capabilities to certain elements and ensure their interoperability (to the extent possible) prior to their release. While new interdependencies and emergent behaviors may arise, the evolution of the SoS should not occur in an ad hoc fashion, constrained by the capabilities of whatever system is produced first. The Integration Working Group must develop schedules that incorporate regular incremental testing of constituent systems, and their interoperability.

  In order to map out an efficient trajectory along which the SoS can evolve, the Integration Working Group should promote the use of architectural tools and prototypes. These tools can be used to anticipate unexpected couplings and avoid the potential for overlooked, underutilized, or duplicated functionalities.
  Testing actual system components is critical, but in order to avoid costly system redesign, testing prior to production is essential. Piaszczyk (2011) writes that existing

tools can be used to great effect to identify and document "the interfaces between hardware, software and humans that constitute the SoS" (p. 3).

- **Strengthen human capital.**

  Successful development of SoS requires the right personnel, but long-term DoD employees often lack the necessary system engineering skills and technical experience. The private sector, which in many respects is well ahead of the government in developing integrated systems, has more people with experience. Consequently, in most cases, the government will have to rely on private firms, which because of their scale, capacity, and flexibility, are better able to provide the necessary SoS engineering. Based on the experience with LSIs, however, the PEO must ensure that organizational conflicts of interest are considered and mitigated when contracting for these integration activities.

  The government, however, must still have sufficient capability to maintain oversight of critical requirements and trade-offs, as well as the source selection of each of the numerous system prime contractors. The government's understaffed acquisition workforce, in many cases, is not adequate to serve these oversight requirements. The DoD must address these human capital needs, in order to successfully develop the required SoSs.

  Accordingly, the DoD must recruit highly qualified systems engineers who have relevant domain experience and have demonstrated a proven ability to operate in complex environments. They must be able to incorporate the effects of time lags and non-linear system interactions into their planning decisions. As mentioned in the previous section, those with professional degrees (e.g., certified engineers) or doctorates are the only segment of the government workforce that, in terms of total compensation, earns less than their private-sector counterparts. Thus, increasing this segment's pay may be critical, especially for those in program oversight and

management positions. A near-term solution is to increase the use of highly qualified experts (HQEs).[5]

- **Provide greater funding flexibility**

  As discussed previously, providing funding at the platform level tends to facilitate system (as opposed to SoS) optimization. Ideally, the Program Leadership Board would be given greater flexibility to allocate and divert funding among individual programs in order to promote the objectives of the SoS. As the SoS evolves, some program budgets may need to be increased, while others will need to be reduced to optimize the effectiveness of the SoS.

## *Conclusion*

SoS acquisition has proven quite challenging. In fact, there are signs that the government may be reluctant to embrace future SoS projects. For example, the failed initial approaches to development undertaken by Deepwater and FCS were replaced with more traditional platform-centric structures. Rather than revise their SoS approach, leadership decided to play it safe in an effort to avoid perceived risk. We contend, however, that generally speaking, an SoS approach is less risky, both technically and financially, especially in light of the potential benefits. Indeed, the JTRS program's initial decentralized approach bears this out—it was, arguably, just as unsuccessful as the SoS approaches undertaken by FCS and Deepwater—which is why JTRS governance was eventually centralized and reorganized under a joint PEO.

We are not suggesting, however, that all of the attributes of platform-centric management be marginalized. In fact, the absence of platform-centric emphasis doomed Deepwater and FCS from the start, leaving requirements unstable, funding inadequate, and physical solutions undefined. At the same time, however, a robust SoS governance structure is necessary to

[5] Section 9903 of Title 5, *United States Code* (U.S.C.), provides the DoD with the ability to recruit experts with state-of-the-art knowledge in fields of critical importance to the DoD. Specifically, the DoD is authorized to develop a program to hire highly qualified experts in critical occupations for up to five years, with the possibility of a one-year extension, at an appropriate level of compensation.

coordinate requirements, budgets, schedules, and modifications in order to successfully deliver the end products.

Our adversaries are working to exploit weaknesses in our current military force structure using whatever means possible. The military must be able to adapt quickly in such an environment. By leveraging the many benefits of integrated, interoperable systems, the U.S. military will be able to successfully counter new threats as they arise.

# References


Abrams, D. & Hogg, M. Hogg. (2010). Social identity and self-categorization. In J. F. Dovidio, M. Hewstone, Glick, P. & Esses, V. (Eds.), The SAGE handbook of prejudice, stereotyping and discrimination (179-193). London, UK: SAGE.

Aerospace Industries Association. (2007, August). *Overcoming barriers to public service*. Retrieved from http://www.aia-aerospace.org/assets/report_barriers.pdf

Alberts, D., Garstka, J., & Stein, F. (2000). *Network centric warfare: Developing and leveraging information superiority.* Washington, DC: DoD C4ISR Cooperative Research Program.

Allison, M., Batdorf, R., Chen, H., Generazio, H., Singh, H., & Tucker, S. (2004). *The characteristics and emerging behaviors of system of systems*. NECSI: Complex Physical, Biological and Social Systems Project. Retrieved from http://necsi.edu/education/oneweek/winter05/NECSISoS.pdf

Ashby, W. (1956). *An introduction to cybernetics*. London, UK: Chapman & Hall.

Attracting highly qualified experts. 5 U.S.C. § 9903 (2006).

Baddeley, A. (2005, March). From cluster to cluster: JTRS makes and rides the waves. *Military Technology*, *29*(3), 74–80.

Boeing Integrated Defense Systems. (2003). Army and Boeing-SAIC LSI team selects Future Combat Systems partners. Retrieved from http://www.boeing.com/defense-space/ic/fcs/bia/nr_030710m.html

Boeing Integrated Defense Systems. (2004). Army, Boeing sign agreement to increase funding for Future Combat Systems program by up to $6.4 billion. Retrieved from http://www.boeing.com/news/releases/2004/q3/nr_040809s.html

Boeing Integrated Defense Systems. (2006). *Future Combat Systems smart book* (FCS case 06-183).

Brewin, B. (2011, May). Defense looks for commercial alternative to its broadband battlefield radio. Retrieved from http://www.nextgov.com/nextgov/ng_20110523_8511.php

Brogan, M. (2007). *Joint Mine Resistant Ambush Protected (MRAP) vehicle program: Lessons being learned*. Quantico, VA: U.S. Marine Corps Systems Command.

Brown, T., Potoski, M., & Van Slyke, D. (2008). *The challenge of contracting for large projects: A case study of the Coast Guard's Deepwater program*. Washington, DC: IBM Center for the Business of Government.

Brown, A., Stricklan, L., & Babich, D. (2006). *Implementing a GPS waveform under the software communication architecture*. Colorado Springs, CO: NAVSYS Corporation.

Button, K. (2010). Why JTRS can't handle UAV video. *Defense News.* Retrieved from http://www.defensenews.com/story.php?i=4441093&c=FEA&s=TEC

Child, J. (2005, May). Future Combat Systems: Shaken up, but not broken up. *COTS Journal*. Retrieved from http://www.cotsjournalonline.com/articles/view/100335

Conant, R., & Ashby R. (1970). Every good regulator of a system must be a model of that system. *Journal of Systems Science*, *1*(2), 89–97.

Carney, D., Fisherman, D., & Place, P. (2005). *Topics in interoperability: Systems of systems evolution*. Integration of Software-Intensive Systems Initiative. Retrieved from http://www.sei.cmu.edu/reports/05tn002.pdf

Crock, S. (2005, August 4). The right stuff for future GIs? A Boeing-led $125 billion program to develop Future Combat Systems is raising eyebrows. Will the weapons make soldiers more vulnerable, not less? *Business Week*. Retieved from http://219.140.69.44:86/magzine/businessweek/businessweek2005-08-15.pdf

Cybernetics. (2009). In *American Heritage Dictionary* (5th ed.). Houghton, Mifflin, Harcourt. Retrieved from http://ahdictionary.com/word/search.html?q=cybernetics&submit.x=0&submit.y=0

Daily, C., Dalton, D., & Cannella, A., Jr. (2003, July). Corporate governance: Decades of dialogue and data. *Academy of Management Review, 28*(3), 371–382.

Defense Acquisition University. (2011). *Defense acquisition guidebook.* Washington, DC: Department of Defense.

Department of Defense & Defense Advanced Research Projects Agency (DARPA). (2002, March 7). DARPA, Army announces Future Combat Systems lead system integrator (No. 109-02) [Press release]. Retrieved from http://www.defense.gov/releases/release.aspx?releaseid=3261

DeLaurentis, D., & Crossley, W. (2005, October). *A taxonomy-based perspective for system of systems design methods* (Paper 925). Paper presented at the IEEE 2005 Conference on Systems, Man, and Cybernetics, Waikoba, HI.

DeLaurentis, D., & Mane, M. (2010, May). *System development and risk propagation in systems of systems*. In *Proceedings of the Seventh Annual Acquisition Research Symposium.* Monterey, CA: Naval Postgraduate School.

Dillard, J. (2008). Organizational aspects of defense acquisitions. In R. Rendon & K. Snider (Eds.), *Management of defense acquisition projects* (pp. 259–265). Reston, VA: American Institute of Aeronautics and Astronautics.

Engwall, M. (2003). No project is an island: Linking projects to context and history. *Research Policy, 32*(5), 789–808.

Erwin, S. (2010, May). Army's iPhone dreams clash with reality. *National Defense Magazine*. Retrieved from http://www.nationaldefensemagazine.org/archive/2010/May/Pages/ArmysiPhoneDreamsClashWithReality.aspx

FCS rolls on, Boeing receives another $219M. (2005, September). *Defense Industry Daily*. Retrieved from http://www.defenseindustrydaily.com/fcs-rolls-on-boeing-receives-another-219m-01249/

Francis, P. (2006). *Defense acquisitions: Business case and business arrangements key for Future Combat System's success* (GAO-06-478T). Washington, DC: Author.

General Accounting Office (GAO). (1999). *Challenges associated with implementing the Joint Tactical Radio System* (GAO/NSIAD 99-179). Washington, DC: Author.

General Accounting Office (GAO). (2003). *Challenges and risks associated with the Joint Tactical Radio System* (GAO-03-879R). Washington, DC: Author.

Goldwater-Nichols Act, 10 U.S.C. § 162 (1986, October 1).

Government Accountability Office (GAO). (2004). *Contract management: Coast Guard's Deepwater program needs increased attention to management and contractor oversight* (GAO-04-380). Washington, DC: Author.

Government Accountability Office (GAO). (2005). *Future Combat Systems challenges and prospects for success.* (GAO-05-428T). Washington, DC: Author.

Government Accountability Office (GAO). (2007a). *Defense acquisitions: Key decisions to be made on Future Combat System* (GAO-07-376). Washington, DC: Author.

Government Accountability Office (GAO). (2007b). *Defense acquisitions: Role of lead systems integrator on Future Combat Systems: Program poses oversight challenges* (GAO-07-380). Washington, DC: Author.

Government Accountability Office (GAO). (2008a). *Defense acquisitions: Assessments of selected weapon programs* (GAO-08-467SP). Washington, DC: Author.

Government Accountability Office (GAO). (2008b). *Status of selected aspects of the Deepwater program* (GAO-08-270R). Washington, DC: Author.

Government Accountability Office (GAO). (2010). *Deepwater requirements, quantities, and cost require revalidation to reflect knowledge gained.* (GAO-10-790). Washington, DC: Author.

Grant, G. (2009, June). It's official: FCS cancelled. Retrieved from http://www.dodbuzz.com/2009/06/23/its-official-fcs-cancelled/

Halchin, E. (2011). *Other transaction (OT) authority*. Washington, DC: Congressional Research Service.

Harrison, T. (2010, January). *Looking ahead to the FY 2011 defense budget*. Washington, DC: Center for Strategic and Budget Assessments.

Hogg, M., van Knippenberg, D., & Rast, D., III. (2012). Intergroup leadership in organizations: Leading across group and intergroup boundaries. *Academy of Management Review*, *37*, 232–255.

Hutton, J., & Caldwell, S. (2008). *Coast Guard: Deepwater program management initiatives and key homeland security missions* (GAO-08-531T). Washington, DC: Government Accountability Office.

Ivory, C., & Alderman, N. (2005). Can project managers learn anything from studies of failure in complex systems? *Project Management Journal*, *36*(3) 5–16.

Joint Program Executive Office, Joint Tactical Radio System (JPEO JTRS). (2011, September). Welcome page. Retrieved from http://www.public.navy.mil/jpeojtrs/Pages/Welcome.aspx

Jones, R. (2007, May). *Capabilities-centric acquisition: A systems of systems view of acquisition management*. In *Proceedings of the Fourth Annual Acquisition Research Symposium*. Monterey, CA: Naval Postgraduate School.

Kaplan, J. (2006). *A new conceptual framework for net-centric, enterprise-wide, SoS engineering.*Washington, DC: National Defense University.

Keating, C., Rogers, R., Unal, R., Dryer, D., Sousa-Poza, A., Safford, R., Peterson, W., & Rabadi, G. (2003). System of systems engineering. *Engineering Management Journal*, *15*(3), 36–45.

Kelman, S. (2012, June). A new approach to collaboration. *Federal Computer Week*. Retrieved from http://fcw.com/articles/2012/06/30/comment-steve-kelman-leading-collaborations.aspx?s=fcwdaily_250612&m=1

Kerzner, H. (2004). *Advanced project management: Best practices on implementation* (2nd ed.). Hoboken, NJ: J. Wiley.

Kopp, C. (2005). Network centric warfare fundamentals—Part 1. *Defense Today*, *4*(1), 40–45.

Kotov, V. (1997). Systems of systems as communicating structures (Hewlett Packard Computer Systems Laboratory Paper, HPL-97-124). Retrieved from http://www.hpl.hp.com/techreports/97/HPL-97-124.html

LaPorte, T. (1994). Large technical systems, institutional surprises, and challenges to political legitimacy. *Technology in Society*, *16*(3), 269–288.

Lipton, E. (2006, December 16). Lawmakers say Coast Guard withheld warning of flaws in cutter design. *New York Times*. Retrieved from http://www.nytimes.com/2006/12/14/washington/14cutter.html

Magnuson, S. (2012, January). Rise of smartphones may sound death knell for old push-to-talk radios. *National Defense*. Retrieved from http://www.nationaldefensemagazine.org/archive/2012/January/Pages/RiseofSmartphonesMaySoundDeathKnellforOldPush-to-TalkRadios.aspx

Maier, M. (1998). Architecting principles for system of systems. *Systems Engineering*, *1*(4), 267–284.

Miller, R., & Hobbs, B. (2005, September). Governance regimes for large complex projects. *Project Management Journal*, *36*(3), 42–50.

Morris, E., Place, P., & Smith, D. (2006). *SoS governance: New patterns of thought*. Pittsburg, PA: Carnegie Mellon Software Engineering Institute.

Munns, D. (2007, August 1). The engineer: Rear Adm. Ronald Rabago takes the helm as the Deepwater program reaches a turning point. *Seapower*. Retrieved from http://www.seapower-digital.com/seapower/200708?pg=34#pg17

National Research Council. (2008). *Pre-milestone A and early-phase systems engineering: A retrospective review and benefits for future Air Force systems.* Retrieved from http://www.incose.org/chesapek/Docs/2010/Presentations/Early-Phase_Sys_Engr-AirForceStudy-NRC_2008.pdf

North, D. (1990). *Institutions, institutional change, and economic performance.* Cambridge, UK: Cambridge University Press.

Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (OUSD[AT&L]). (1996). *The DoD integrated product and process development handbook*. Washington, DC: DoD.

Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (OUSD[AT&L]). (2007). *System of systems engineering guide: Considerations for systems engineering in a system of systems environment.* Washington, DC: DoD.

Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (OUSD[AT&L]). (2008). *Systems engineering guide for systems of systems*. Washington, DC: DoD.

Owens, W. (1996). The emerging U.S. systems-of-systems. *Strategic Forum 63*. Institute for National Strategic Studies, National Defense University. Retrieved from http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA394313

Parchem, A., & Gowing, M. (2009, May). Improving government: Accelerating the impact of new political-career executive teams. *Federal News Radio*. Retrieved from http://www.federalnewsradio.com/?nid=&sid=1678133

Perrow, C. (1984). *Normal accidents: Living with high risk technologies.* New York, NY: Basic Books.

Perrow, C. (1999). *Normal accidents with an afterword and postscript on Y2K*. Princeton, NJ: Princeton University Press.

Piaszczyk, C. (2011, May). Using architectural tools to reduce the risk in systems-of-systems integration. In *Proceedings of the Eighth Annual Acquisition Research Symposium*. Monterey, CA: Naval Postgraduate School.

Pincus, W. (2012, June 13). The battle for the military's future. *The Washington Post.* Retrieved from http://www.washingtonpost.com/world/national-security/the-battle-for-the-militarys-future/2012/06/13/gJQAZIxxaV_story.html

Sage, A., & Cuppan, C. (2001). On the systems engineering and management of systems of systems and federations of systems. *Information Knowledge Systems Management*, 325–345.

Scales, R. (2006). *Future Combat Systems: Its origin and operational concept*. St. Louis, MO: Boeing Integrated Defense Systems.

Scholten, D. (2012, January 3). Every good doctor must represent the patient: The failure of evidence-based medicine. *Orthomolecular Medicine News Service*. Retrieved from http://www.theoneclickgroup.co.uk/news.php?id=6744" \l "newspost"

Sengupta, Abdel-Hamid, & Van Wassenhove. (2008, February). The experience trap. Harvard Business Review, *86*(2), 94-101.

Sisti, F., & Latimer, D. (2007). Linking leadership and technical execution in unprecedented systems-of-systems acquisitions. *Society for Design Process Science*, *11(2)*.

*The United States Coast Guard Deepwater program: Statement of Richard L. Skinner Inspector General, U.S. Department of Homeland Security, before the Subcommittee on Oceans, Atmosphere, Fisheries and Coast Guard Committee on Commerce, Science, and*

*Transportation, United States Senate,* 110th Cong. (2007). Retrieved from http://www.oig.dhs.gov/assets/TM/OIGtm_RLS_021407.pdf

Smith, R. (2005*). The utility of force: The art of war in the modern world*. New York, NY: Knopf.

Stevens, R. (2004). *Engineering enterprise systems: Challenges and prospects*. McLean, VA: The MITRE Corporation.

Thomas, J., & Buckle, P. (2004, August). Exploring the gendered logic systems in project managers' discourse. In *Proceedings of the IRNOP VI Project Research Conference*, Turku, Finland: IRNOP.

Toenjes, S. (2008, April). Safeguarding against organizational conflict of interest (OCI) on the Future Combat Systems (FCS) programs. *Army AL&T,* 48–50.

U.S. Army. (2007). *Future Combat Systems (brigade combat team) white paper* (GOVT 07-028).

# Acknowledgements

This research was sponsored by the Naval Postgraduate School, and we are especially grateful for the support and encouragement provided by Rear Admiral Jim Greene (USN, Ret.) and Keith Snider. We would also like to acknowledge Kenneth Holland and Michael Garber, graduate students at the University of Maryland's School of Public Policy, whose research contributed to this report. Finally, we would like to thank our co-worker Caroline Dawn Pulliam for her assistance with the planning and coordination of this study.

# 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 1997–2001, Dr. 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, Dr. 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), senior vice president at TASC, vice president of ITT, and engineering and management positions with Singer and Raytheon Corporations.

Throughout his career, Dr. 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, Dr. 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 (GAO) 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, he served as interim dean of the School of Public Policy at the University of Maryland and from 2004–2006, Dr. Gansler 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 at the 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.

His 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, Mr. 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, Mr. Lucyshyn completed a 25-year career in the U.S. Air Force. Mr. 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.

**John Rigilano**

John Rigilano is a faculty research assistant at the Center for Public Policy and Private Enterprise. He earned his Master of Public Policy degree from the University of Maryland, College Park in 2011, and holds a Bachelor of Arts degree in anthropology from the Pennsylvania State University. He is pursuing a career in policy and program analysis.

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.