Lessons Learned: Building a New National Intelligence Partnership

A White Paper prepared by the AFCEA Intelligence Committee

April 2006

AFCEA

The Association committed to serving Intelligence Professionals

Intelligence, Technology, and Integration – Building the Intelligence Enterprise

Table of Contents

Copyright 2006 by AFCEA International
Reproduction permitted with appropriate citation

Executive Summary

This is the fifth in a series of white papers by the Armed Forces Communications and Electronics Association (AFCEA) Intelligence Committee contributing to the national discussion on the future of our nation's intelligence capabilities. This paper examines issues relating to the challenge of the development and acquisition of technology in support of the Intelligence Community's evolving global mission. It does so in the context of the Intelligence Reform and Terrorism Prevention Act of 2004, the vision embodied by the National Intelligence Strategy, and the recent work of the Defense Acquisition Performance Assessment (DAPA) report.

The paper focuses on the development, acquisition, and insertion of needed technology. It addresses issues surrounding three important challenges facing the Intelligence Community:

1 A technology development and acquisition capability (policy, process, workforce, etc.) necessary to support the increasing Community role in gaining the operational scale required to master today's global intelligence environment
2 The creation and deployment of an integrated architecture capable of serving the needs of the Intelligence Community, as defined by the Director of National Intelligence (DNI)
3 Mechanisms and reliable structures to identify, develop, acquire, and insert new and promising technologies into the Community's existing inventory.

To meet these challenges, this paper and the Intelligence Committee make three over-arching recommendations. These steps can be taken today and will yield dramatic results:

1. To allow for the acquisition and insertion of the needed technologies, the Intelligence Community should develop and implement a truly integrated intelligence architecture, implemented in large part by a unified corps of architecture, systems engineering, and acquisition professionals. Such architecture will benefit both the Intelligence Community and the larger national security community of which it is a part. The work of the newly appointed Chief

Copyright 2006 by AFCEA International
Reproduction permitted with appropriate citation

Information Officer (CIO) to undertake this effort with regard to information technology is a good first step. The CIO's efforts should be broadly supported and used as a model for a broader, unified architecture**.** To facilitate this, the Community should work with Congress and the Defense Department to create an atmosphere in which risk and risk management are encouraged more broadly.

2. The tremendous successes of the past resulted directly from a unique partnership between the Intelligence Community and the private sector. In the past, the government was the source of most technological innovation. Today, much of the innovation required exists in the private sector, developed for non-governmental purposes. As a matter of priority, therefore, the Intelligence Community should take the steps necessary to build, renew, and/or rekindle a partnership between the public and private sectors, one based on trust, development of the industrial base requisite to building new capabilities, and sound business practices.
3. The Intelligence Community should put in place a unified process for the rapid and agile development and acquisition of new and emerging technologies. The recent actions by the Associate Director of National Intelligence for Science and Technology are good first steps, but they must, as is true for the efforts of the CIO, be applied more broadly as part of a coherent architecture and plan. These steps, such as the realignment of the Advanced Research and Development Activity (ARDA), are consistent with the Committee's earlier recommendations in its second white paper (October 2004) regarding the development of a strong intelligence workforce, improved architectural discipline, and greater emphasis on the creation of a national industrial base in support of our nation's vital intelligence needs.

Beyond the focus of this paper, but certainly relevant to the theme being addressed, are other needed reforms, including those relating to organization, budget authority, workforce development, and the requirements process. Some of these issues are addressed in earlier AFCEA white papers; others will be addressed in subsequent papers. Many issues have been and will be the subject of needed debate as the Community goes forward. AFCEA and the Intelligence Committee look forward to contributing to this

Copyright 2006 by AFCEA International
Reproduction permitted with appropriate citation

debate, including participation in further development of the needed government partnership with the private sector.

Introduction

The Intelligence Committee (the Committee) of the Armed Forces Communications and Electronics Association (AFCEA) is pleased to present this fifth in a series of white papers[1] focused on the future of the Intelligence Community (the Community). The Committee's development of these papers, and the AFCEA Intelligence Symposia they accompany, are intended to contribute substantively to the national discussion on the strengthening our nation's intelligence capabilities. The Committee is aware of changes taking place in the user community, in the development of intelligence priorities, among the leadership of the Community, and in the underlying operational concepts by which intelligence is made organic to the pursuit of our national interests. In addition, AFCEA and the Committee are very sensitive to the comparable pressures and changes facing the private sector, factors that must be addressed if the Community is to be successful going forward. These white papers and symposia are intended to support those changes in a manner as dynamic as the changes themselves. As with our most recent white paper, the Committee is circulating this paper to speakers, panelists, and other participants in advance of the next Intelligence Symposium. We are doing so to provide a common frame of reference for symposium discussions with respect to issues the Committee believes are of vital importance to the future of intelligence.

Within the context of the 2006 AFCEA Spring Intelligence Symposium, this white paper highlights three specific challenges facing the Community with respect to developing and acquiring the requisite technology. The Committee believes these challenges can be met only by broad Community acceptance of new initiatives by the DNI. The key challenges are:

1 Creating an integrated architecture of requirements, resources, programs, and capabilities that supports the vision framed recently by the National Intelligence Strategy of the United States of America, a strategy "*to integrate, through*

[1] For previous white papers, see: http://www.afcea.org/committees/intel/intelwhitepaper.asp

Copyright 2006 by AFCEA International
Reproduction permitted with appropriate citation

intelligence policy, doctrine, and technology, the different enterprises of the Intelligence Community."

2 Strengthening the partnership between the public and private sectors to ensure the Community's future capabilities will reflect the strongest possible contributions of our nation's industrial base.

3 Identifying and putting in place the mechanisms for technology acquisition and insertion into the Intelligence Community that allow advanced technology both to be acquired effectively and efficiently and to be deployed at a rate as dynamic as that at which the technology itself is developed and made available.

The effective and efficient acquisition of technology and capabilities vital to the national security is a challenge common to both the defense and intelligence communities. The Intelligence Committee, therefore, commends the DAPA report, published in January 2006, as both a source of valuable insight into these challenges and as a source of ways to address the challenges successfully. The Intelligence Committee fully understands that some of the acquisition and technology challenges facing the Intelligence Community are unique to that Community as opposed to the larger national security community of which the Intelligence Community is a vital part. Regardless, the DAPA report speaks to issues and concerns relating to defense programs that are applicable to many Intelligence Community initiatives. Given that the Community uses, to some extent, the acquisition methodologies used by the Department of Defense (DOD) and shares in DOD milestone decision authority for some intelligence programs, we believe lessons applicable to DOD are also pertinent to the Intelligence Community.

Building a System of Systems: Intelligence Community Technology and Acquisition Challenges and Opportunities

The need for a strengthened technology acquisition capability serving the nation's intelligence capabilities has never been greater. No matter how it is characterized, the overarching challenge of creating an intelligence capability that scales to the global intelligence environment and meets the needs of the National Intelligence Strategy "*to integrate, through intelligence policy, doctrine, and technology, the different enterprises*

Copyright 2006 by AFCEA International
Reproduction permitted with appropriate citation

of the Intelligence Community" requires our best efforts.

While one could point to real and imagined deficiencies in the acquisition of intelligence capabilities, it is also useful to bear in mind that the Intelligence Community has acquired unmatched capabilities over time—and has done so as a reliable counterpart to a defense community that has acquired technical systems of unprecedented capability and effectiveness. At all levels, U.S. intelligence capabilities reflect impressive imagination, scope, and robustness. Far from decrying the Cold War attitude often associated with the Intelligence Community, the Intelligence Committee views the achievements of the Community during and after the Cold War as positive lessons to be learned and applied in the present. Working with industry, the Community provided U.S. decision-makers and war-fighters with incomparable advantages. It did so swiftly, building on industrial relationships and contract mechanisms flight-tested during the World War II, such as parallel development, cost plus contracts, and a deliberate investment in the industrial base necessary to provide the technologies and systems vital to national intelligence. Although our nation requires technologies and systems that go beyond those acquired in prior decades, many of the challenges faced in those decades, and the approaches to overcome them, remain relevant today. As a result, the Intelligence Committee is optimistic that today's technology and acquisition challenges and problems can be met successfully and that some ideas of the way forward can be found in the past. It is important to note, however, that the balance of technology development has shifted clearly from a situation in which the government primed the pump, as in World War II, to one in which the private sector is already a source for a greater proportion of relevant technology. Such a situation underscores the need to build the stronger industrial relationships for which this white paper calls.

Nonetheless, the challenges facing the Community are significant, and they cannot be solved in isolation: They must be viewed as an integrated portfolio, addressed and resolved simultaneously.

First, the Intelligence Community remains hobbled by the extent to which a common

Copyright 2006 by AFCEA International
Reproduction permitted with appropriate citation

architecture does not exist within individual agencies, much less across the Community, even with regard to common issues. Some are taking steps in recognition of this, but more needs to be done. We acknowledge that the Community's Office of the Chief Information Officer (CIO) (within the Office of the Director of National Intelligence) has made laudable strides in the articulation of a common information architecture in support of IT-enabled mission capabilities Community-wide. Implementation of that architecture— as it exists and as it is evolving—is hindered because architecture and systems engineering, Community-wide, are not unified.

The CIO's promulgation of an IT architecture can only be made real if the implementation of a system of systems is realized through an effort with synchronized standards, schedules, interfaces, risks, and dependencies across the various major capabilities being developed by the Community's components. At the Community level, the architecture and systems engineering disciplines are not yet unified; similarly, neither systems engineering nor architecture is unified across the variety of disciplines (collection, exploitation analysis, production, dissemination, mission management, etc.) that compose the intelligence value chain. The Committee understands the perceived need for sufficient flexibility at the individual agency level to pursue and deploy new technologies and systems with speed and agility, unhindered by a cumbersome bureaucracy. Still, an integrated Community requires systems that work together, and achieving this implies that they were *meant* to work together. A unified systems engineering approach, applied Community-wide, coupled explicitly to Community architecture, represents the best chance in the near term of gaining the integrated capabilities required to scale up to the global intelligence environment.

Realizing an integrated system of systems—one reflecting an integrated intelligence enterprise—also requires that architecture and systems engineering be made more authoritative by the application of Community-wide acquisition approaches and authorities. The Intelligence Reform and Terrorism Prevention Act of 2004 vests the DNI with milestone decision authority for major acquisition systems. Under "Acquisitions of Major Systems," the Act states:

Copyright 2006 by AFCEA International
Reproduction permitted with appropriate citation

"*(1) For each intelligence program within the National Intelligence Program for the acquisition of a major system, the Director of National Intelligence shall—*

(A) Require the development and implementation of a program management plan that includes cost, schedule, and performance goals and program milestone criteria, except that with respect to Department of Defense programs the Director shall consult with the Secretary of Defense;

(B) Serve as exclusive milestone decision authority, except that with respect to Department of Defense programs the Director shall serve as milestone decision authority jointly with the Secretary of Defense or the designee of the Secretary."

Under "Intelligence Information Sharing," the Act also states:

"(1) The Director of National Intelligence shall have principal authority to ensure maximum availability of and access to intelligence information within the intelligence community consistent with national security requirements. The Director of National Intelligence shall—

(A) Establish uniform security standards and procedures;

(B) Establish common information technology standards, protocols, and interfaces;

(C) Ensure development of information technology systems that include multi-level security and intelligence integration capabilities;

(D) Establish policies and procedures to resolve conflicts between the need to share intelligence information and the need to protect intelligence sources and methods;

(E) Develop an enterprise architecture for the intelligence community and ensure that elements of the intelligence community comply with such architecture; and

(F) Have procurement approval authority over all enterprise architecture-related information technology items funded in the National Intelligence Program."

Copyright 2006 by AFCEA International
Reproduction permitted with appropriate citation

The preceding demonstrates that Congress clearly recognizes the need to unify architecture, engineering, and acquisition at the Community level. To the extent that impediments to this unification exist, they limit progress toward the integrated Community explicit in the DNI's National Intelligence Strategy. At a minimum therefore, exercising the DNI's authorities in support of a unified IT architecture and ensuring that IT systems in general— and those that support mission in particular— conform to that architecture, are roles that the CIO should undertake. This model, if successful, should be applied across the Community in all aspects of acquisition and engineering.

A second challenge impeding Community technology acquisition is the extent to which the Community-wide acquisition and program management corps remains under-strength and disunited. As a result, there is a lack of congressional confidence in the ability of the Community either to achieve important objectives or to confront and manage the risk associated with deploying significant new capabilities. An industrial strength national intelligence capability requires acquisition and program managers equipped with the technical understanding, experience in working with the national industrial base, and authority necessary to achieve the operational scale requisite to master today's intelligence environment. If authority, responsibility, and accountability are not present in the same person, the problems faced today are inevitable.

The Intelligence Committee looks to the examples of the acquisition and program management deployed by the Community during the CORONA program and in the development of the national signals intelligence infrastructure that proved so effective during and after World War II. Technically proficient program managers, equipped with real acquisition authority, accountability, responsibility, and resources and supported by a well-trained cadre of business managers, were able to put in place the acquisition program management structures that were robust, efficient, and rapid in furnishing results. Such teams gained the sustained confidence of the leadership in both the Executive and the Legislative branches. Reconstituting and training such an acquisition cadre, and reflecting its importance as a discreet and important career field within the

Copyright 2006 by AFCEA International
Reproduction permitted with appropriate citation

Community, would allow the DNI both to fulfill the mandate of the Intelligence Reform and Terrorism Prevention Act and to gain the capabilities required for the integrated Intelligence Community. The extent to which major intelligence systems have proved difficult to develop, acquire, and deploy in recent years is evidence of the extent to which this mandate is required.

A third challenge—linked closely to the need for strong acquisition program management—is a capable industrial base. Deficiencies in the industrial base serving the Community are, in part, responsible for major acquisition system delays and other difficulties. These deficiencies are the responsibility of the Community and the industrial base itself. As the Community's resources were constrained in the early 1990s, the view and role of Systems Engineering and Technical Assistance (SETA) within industry changed: SETA was seen less as a source of technology and key technical program management and more as a labor pool (providing bodies where there were insufficient government resources). The resulting Community preference for time and materials contracts shifted programmatic responsibility from vendors to the government. Contractor personnel joined government-led product-teams that focused in most cases on specific problems. The industrial base serving the Community lost, or transferred elsewhere, its capacity to manage major acquisition programs, even as it restructured its resource base to supply the government with cleared personnel assigned to augment the government's own staff. As the Community began in recent years to retool its baseline capabilities, it attempted to do so with an industrial base that was without sufficiently robust program management skills pertinent to major acquisition systems.

The need for a vibrant industrial policy that contributes to the development of the industrial base requisite to new, complex programs is not without precedent. Rear Admiral Hyman G. Rickover, USN, as Director of the Naval Reactors Branch in the US Navy's Bureau of Ships, recognized this phenomenon in the 1950s when he contracted for prototype nuclear submarines in advance of the order of nuclear submarine classes. Each prototype demonstrated a different aspect of technology (alternative reactor designs, platform sizes, sensors) relevant to the deployment of a nuclear submarine force. Each

Copyright 2006 by AFCEA International
Reproduction permitted with appropriate citation

prototype also gave the shipyard building it an opportunity to strengthen its management, technical base, and infrastructure before it received a production order. Delays and difficulties experienced in the delivery of these prototypes contributed to the understanding of the Navy and of the industrial base of the challenges associated with a new technology. By the time the Navy was ready to order its fleet of attack and ballistic missile submarines, it had in place an industrial base capable of providing it. Today, the Intelligence Community and Congress need to regain the capacity to undertake small, medium, and large-scale prototypes or technology demonstration platforms in advance of major acquisition, with the understanding that delays, risks, and other difficulties that surface in the conduct of these precursor activities help both the Community and its industrial base prepare for successful acquisition programs. At the same time, the private sector should redouble its efforts to invest in the program and technology management capabilities required to deliver major acquisition programs, making good on the lessons learned in recent years.

While one could identify other issues, these three over-arching challenges are at the core of the impediments faced by the Community as it seeks to retool itself in the face of the global intelligence challenge.

In spite of the challenges, reasons for optimism exist. As noted above, the Community can credit itself with many successes, and the Committee believes strongly that it can regain the technology acquisition capabilities associated with those successes. In addition, The Honorable Dale W. Meyerrose, Associate Director of National Intelligence and Chief Information Officer, has made clear his commitment to an effective, binding Community IT architecture. This is a necessary step, and with support from the Community's leadership and Congress, we believe his efforts should bear fruit in the development of the integrated capabilities the DNI's vision requires.

Building a New Partnership

The Department of Defense is also seeking to rejuvenate and reform its ability to develop, acquire, and deploy new technologies and systems in a timely fashion to support

Copyright 2006 by AFCEA International
Reproduction permitted with appropriate citation

the transformation-oriented operational concepts reflected in the Joint Transformation Roadmap and other transformational doctrine. The DAPA report highlights many of the problems, issues, and solutions that must be overcome to be successful, most of which are pertinent to the Intelligence Community. Indeed, some of the issues facing DOD apply directly to the Intelligence Community inasmuch as the Community must support defense transformation.

The DAPA report speaks to the need to rebuild partnerships and trust, both within the semi-autonomous organizations involved in the DOD acquisition, requirements, and budgeting processes and with the industry that must deliver the needed new technologies. The DNI must likewise establish the sense of partnership and trust among the various elements of the Intelligence Community, and the Community must then do the same with its industrial base. Foremost among the steps needed to build a new sense of partnership with the private sector is recognition that the industrial base itself is organic to the Community. Lessons pertinent to program management must be common to both government and industry members of the Community. Indeed, the stakes are high for both public and private sectors in building the industrial base capable of developing and delivering new capabilities.

In particular, the DAPA report points to the need for reinvigorating the trust between the public and private sectors. While customers and vendors derive value from different sides of a business transaction, the most valuable relationships take place among customers and vendors that have confidence in each other. Vendors need to trust that their customers both understand their own needs and clearly articulate those needs in the terms of the contract. For their part, customers must believe that vendors are committed to their contractual obligations. This particular insight of the DAPA report is equally true for the Intelligence Community. Building a more trusting relationship, however, depends on the government re-establishing stable organizational alignments and responsibility for key programs as well as stable requirements baselines against which industry can provide solutions.

Copyright 2006 by AFCEA International
Reproduction permitted with appropriate citation

On the government side, acquisition executives who have sufficient resource and budget authority to maintain multi-year program stability are best able to build and exercise a fruitful industrial partnership. Programs that must fight year to year for survival, that are forced to adjust budget profiles to fit annual budgetary realignments and exigencies, make difficult the creation of a partnership with industry that grows stronger and more reliable over a program's lifetime.

The DAPA report provides a great number of detailed recommendations, the bulk of which are beyond the scope of this brief paper. Still, the report's call for program managers appointed by, and responsible to, acquisition executives is particularly relevant to the Intelligence Community. Adopting such an approach would provide industry with recognized and empowered representatives with whom to do business. At the same time, such program managers could form the core of a revitalized acquisition workforce. Such a workforce, in turn, would give both government mission managers and industry partners, alike, confidence that programs are more likely to be executed competently. Consequently, the Intelligence Committee renews its recommendation that the Community establish and maintain a Community-wide acquisition workforce, subject to consistent training, credentials, and performance measures. Such a move should accompany application across the Community of a consistent set of acquisition methodologies, including requirements, test, and evaluation; independent verification and validation (IV&V); and other disciplines.

Agile Technology Acquisition and Deployment

The preceding sections put forth the Committee's view of the need to build a stable acquisition workforce and stable architecture and systems engineering approaches. We urge the Community to take active steps (for example, building stronger, incentives-based contracts; creating a more robust acquisition workforce) to revitalize the public/private sector partnership, thereby strengthening the nation's intelligence capabilities over the long term. Additionally, we view these steps as prerequisites to the agile acquisition and rapid deployment and insertion of new and emerging technologies. The Committee believes that a stable, well-trained, and recognized workforce of

Copyright 2006 by AFCEA International
Reproduction permitted with appropriate citation

architects, systems engineers, and acquisition executives will provide the Community with a corps of professionals capable of moving swiftly both to capture new technological opportunities and to bring to the attention of mission managers technologies for which requirements may not have been defined. A stable architecture makes easier the adoption of new technologies; well-understood information and engineering standards provide government and industry with an environment to which new technologies can be more swiftly adapted.

At the same time, the Community should choose and adopt a set of discreet technology acquisition and development methodologies based principally on their ability to meet the demands for rapid insertion in an environment that puts a premium on swiftness and agility. Today's Intelligence Community is characterized by a variety of rapid acquisition approaches, many of which are unique to individual agencies. The Committee is aware of steps being taken by the Associate Director of National Intelligence for Science and Technology to build a fellows program and align advanced research and development activities at the Community level. We encourage these steps and others that can provide the DNI the means to identify high-potential technologies, make these technologies available across the Community, and develop and acquire the technologies swiftly without recourse to agency-specific acquisition requirements. The Community needs comparable efforts and methods for rapid technology insertion.

Summary

This white paper provides an overview of the challenges and problems faced by the Intelligence Community in technology development and acquisition. It also provides a high-level view of the ways in which these challenges and problems might, over time, be addressed and overcome. The DAPA report provides a more detailed view of the problems facing the larger national security community as well as a broad set of recommendations. The recommendations in this white paper are a selected subset of those from the DAPA report. This paper focuses, however, only on those high-level needs that must be addressed first. The Committee urges the Director of National Intelligence and the Intelligence Community to build the integrated architecture, systems

Copyright 2006 by AFCEA International
Reproduction permitted with appropriate citation

engineering, and acquisition cadres necessary to achieve an integrated mission infrastructure. Over time, such an infrastructure would provide the robust environment needed to deploy an ever-evolving range of new technologies, while giving the Community the operational scale needed to master the global intelligence environment.

Achieving long-term progress in the face of short-term exigencies is a significant challenge in its own right, a challenge all too easy to set aside. Neither rebuilding our national intelligence capability nor achieving the integrated Intelligence Community to which the Director of National Intelligence has committed his team allows us the luxury of taking the short view. The AFCEA Intelligence Committee stands ready to place its shoulder to the wheel—with the DNI, the Community, and industry — to realize the intelligence capabilities on which our nation depends.

Copyright 2006 by AFCEA International
Reproduction permitted with appropriate citation