Intelligence and the New National Security Environment

A White Paper prepared by the AFCEA Intelligence Committee

OCTOBER 2004

AFCEA

The Association committed to serving the Intelligence Professional

Intelligence and the New National Security Environment

Executive Summary

This paper is the second presented by the Armed Forces Communications and Electronics Association (AFCEA) to help the United States improve the overall capability of the national Intelligence Community independent of organizational structure or architecture.[1] It makes several recommendations that the Committee believes can contribute toward that objective, including:

- Designing a capability organic to the Intelligence Community for new/advanced concept and doctrine development
- Creating and sustaining development of a unified national intelligence service according to unified and consistent standards
- Establishing unambiguous incentives for the development by senior managers of cross-community expertise and understanding
- Creating a capability to organize the Intelligence Community for continuous study of intelligence organization, processes, and operations
- Developing a unified intelligence architecture
- Establishing a unified architecture, engineering, and acquisition organization reporting to a National Intelligence Director to implement a unified intelligence architecture
- Taking initial steps toward consolidated infrastructures for collection and analysis
- Initiating a new government–industry partnership to enhance security management and improve industry's capacity to deploy resources responsive to Intelligence Community needs and timelines.

The AFCEA Intelligence Committee is aware of the vigorous national discussion underway regarding the future of intelligence, the Intelligence Community, and the role of intelligence in national security. Our recommendations are intended to help the new leadership of the Community implement the emerging mandate to create a national intelligence capability giving decision makers the most relevant and accurate intelligence available to any nation—intelligence that is always timely to whatever decisions are faced by our nation's leadership. This paper is presented against the backdrop of challenging national security conditions, the global war on terror, the rise of new state and non-state competitors, an increasingly interconnected global community, rapidly changing technology that both enhances and impedes the collection and analysis of critical intelligence, the ongoing work of the President's Commission to study intelligence related to weapons of mass destruction (WMD), and the findings and recommendations of the 9/11 Commission.

At the core of the Committee's recommendations is development of a top-down concept for integrated intelligence, coupled with creation of capabilities organic to the Intelligence Community to study the future of intelligence and to help develop new concepts and doctrines. This capability is analogous to some extent to the capabilities employed by the armed services, capabilities they have employed to help transform themselves and undertake the revolution in military affairs.

---

[1] See the previous paper at: http://www.afcea.org/downloads/HIWhitePaper.pdf. That paper is focused principally on near-term opportunities to achieve functional integration using contemporary information technology, while remaining largely within today's organizational context.

In response to the need for an intelligence capability that provides intelligence consumers with integrated products that "connect the dots," regardless of the discipline (IMINT, HUMINT, MASINT, SIGINT, etc.) by which the underlying data is collected, our recommendations encompass an approach to unified collection and analytic infrastructures. Building such infrastructures and creating an integrated intelligence "system of systems" comprised of interoperable components requires a unified architecture and a consistent engineering approach. Ensuring that such an architecture and engineering approach is reflected in each component of the new national intelligence capability is most likely if the acquisition of these components is within the authoritative oversight of a Community-wide director of technology, architecture, engineering, and acquisition. Such a director must be vested with the authority, resources, and mechanisms commensurate with the serious, Community-wide responsibilities associated with building an effective system-of-systems scaled to the global intelligence challenge.

A new national intelligence capability can be no stronger than its most important component—its workforce. To that end, the Committee recommends the creation of a national intelligence service equipped with powerful incentives that couple senior advancement to Community-wide experience and demonstrated commitment to an integrated, Community-wide perspective. We also recommend implementation of an integrated approach to professional and career development, linked closely to the underlying principles of an integrated Intelligence Community.

Finally, the Committee's industry representatives urge the nation to pay special attention to rebuilding the government-industry partnership that created the national intelligence capabilities that helped the United States win the Cold War. We look to the Community for a strengthened approach to security management, one that allows both government and industry increased flexibility in the deployment of vital human resources against our most challenging intelligence problems. We look to the Community as well for more consistent approaches to acquisition – approaches employed by a Community-wide acquisition corps equipped with an acquisition methodology that provides both the discipline necessary for deployment of integrated capabilities and the responsiveness needed to address dynamic intelligence challenges.

We are aware that some of these recommendations echo those made by other commentators. In adding our voice to theirs, the Committee desires to make more visible a vision of national intelligence in which integrated capabilities are developed and sustained at the level of excellence our citizens expect and deserve.

Building a new national intelligence capability is a challenge of the scale to which our nation invariably rallies and at which our nation is invariably successful. Like the Manhattan Project and the successful effort to reach and return from the moon, this is a challenge that can be met only by keeping in view our objective—measuring each day not how far we've come from our starting point, but how much closer we are to our goal. The goal of building a national intelligence capability, scaled to the global intelligence challenge, able to help protect our nation in an ever more-challenging world, is as important an undertaking as we can imagine. The AFCEA Intelligence Community knows that our nation can meet this challenge. We believe it will.

Intelligence and the New National Security Environment

TABLE OF CONTENTS

1. Overview and Purpose in Presenting this Paper—The Government Industry Partnership:

This paper is the second in a series of papers presented by the Intelligence Committee of the Armed Forces Communications and Electronics Association (AFCEA). This paper focuses on key steps needed to improve the overall capability of the national Intelligence Community independent of organizational structure and architecture. It makes several recommendations the Committee believes can contribute toward that objective, including:

- Designing a capability organic to the Intelligence Community for new/advanced concept and doctrine development
- Creating and sustaining development of a unified national intelligence service according to unified and consistent standards
- Establishing unambiguous incentives for the development by senior managers of cross-community expertise and understanding
- Creating a capability to organize the Intelligence Community for continuous study of intelligence organization, processes, and operations
- Developing a unified intelligence architecture
- Establishing a unified architecture, engineering, and acquisition organization reporting to a National Intelligence Director to implement a unified intelligence architecture
- Taking initial steps toward consolidated infrastructures for collection and analysis
- Initiating a new government–industry partnership to enhance security management and improve industry's capacity to deploy resources responsive to Intelligence Community needs and timelines.

The Committee presents these papers to contribute substantively to the national discussion underway regarding the future of intelligence, the Intelligence Community, and the role of intelligence in our national security. The Committee hopes the recommendations it presents complement other efforts to build a national intelligence capability that meets the nation's needs. The Committee is aware that the national discussion regarding the future of intelligence is taking place against the backdrop of challenging national security conditions, the global war on terror, the rise of new state and non-state competitors, an increasingly interconnected global community, rapidly changing technology that both enhances and impedes the collection and analysis of critical intelligence, the ongoing work of the President's Commission to study intelligence related to weapons of mass destruction (WMD), and the findings and recommendations of the National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission).

The previous paper (see: http://www.afcea.org/downloads/HIWhitePaper.pdf) focused principally on near-term opportunities to achieve functional integration using contemporary information technology, while remaining largely within today's organizational context. In addition, the earlier paper identified the legal and statutory bases for today's intelligence structure, including those components that would have to be addressed should the President and Congress undertake significant organizational reform. Finally, the earlier paper endorsed (by reference) work undertaken by the Security Affairs Support Association (SASA) and others to identify potential changes that could help enable the integration in Intelligence Community security. The AFCEA Intelligence Committee renews its endorsement of those recommendations, given the need to build a skilled, flexible, and deployable industrial capability to help the United States meet its intelligence needs.

In this paper, the Intelligence Committee builds on the earlier paper and takes aim at specific steps that can be taken by the executive and congressional branches, regardless of the manner in which 9/11 Commission recommendations and other recommendations are accepted by the President and Congress. AFCEA offers this paper in service to the reinvigoration of the government–industry partnership that has been the hallmark of our national defense capabilities since World War II. Within the Intelligence Community, that partnership has been made substantially less effective by continued stove piped security processes that make difficult the effective allocation of skilled human resources; by security investigation backlogs that impede the ability of the nation's scientists, engineers, and technologies to aid in the development of a true national intelligence capability; by lack of system architecture, slowing the pace of advanced information technology insertion and enterprise operations; and by inadequate engineering and acquisition oversight capable of creating a true "system of systems" for an Intelligence Community capable of meeting this nation's expectations. The Committee's recommendations touch on these subjects, as well as on issues relating to human resource management and the creation of intelligence concepts and doctrine appropriate to the evolving national security environment. The recommendations take advantage of our nation's competitive advantages in ever-more-capable technologies and processes available from the nation's industrial base.

A Word About Scope—The Committee recognizes that this paper does not encompass the full range of questions that will influence the development of a stronger national intelligence capability. We believe that a stronger intelligence research and development (R&D) capability, for example, is an important aspect of rebuilding national intelligence. Likewise, we see the deployment of stronger intelligence research capabilities, including the application of new technology and tools to ever-more complex intelligence problems, as important to this effort. Similarly, we recognize that financial management, and possibly the creation of a common financial management cohort, is a subject worthy of detailed discussion. The Committee expects to address these and other subjects pertinent to the future of intelligence in subsequent white papers corresponding to future AFCEA Intelligence Symposia.

2. The Philosophy of Change—Getting to the Future

The wake of the terrorist attacks on September 11, 2001, has led to a profound sense in the public, on Capitol Hill, and in other quarters that the nation can—and must—do substantially better if it is to protect itself and advance its national interests in an increasingly complex international environment. The controversy surrounding the nation's ability to detect weapons of mass destruction (WMD), continuing hostilities in Iraq, and enduring concerns about terrorism threatening not only U.S. interests abroad, but also here at home, all serve to amplify concerns over national intelligence capabilities. At the same time, the nation continues to face other intelligence challenges. International economic competition to the United States, changes in the U.S. debt position (and our dependence on foreign creditors), foreign programs to develop advanced weapons, tensions on the Korean Peninsula, and China's emerging global reach are some of the concerns likely to remain with us for many years. Some of these issues may account for long-term components of the national intelligence infrastructure, even as our traditional concern with the Soviet Union led to a worldwide infrastructure of resources dedicated to watching and assessing the capabilities and intentions of our principal peer-competitor during the Cold War. As a result, the investment the nation is likely to make in building a new national intelligence capability could be substantial—in the hundreds of billions of dollars over the next few years— raising the stakes for the decisions we take today.

As Americans, we have met other, vital challenges to our national security. The United States rose to the challenge of World War II by creating entirely new disciplines of industrial organization, operations research, and systems analysis. American military planners and logisticians revolutionized the means by which forces were created, deployed, and supported. American scientists (and foreign scientists drawn to America's scientific culture) solved a number of fundamental problems in science and technology, leading to the deployment of nuclear energy. The launch of *Sputnik* and the Soviet manned spaceflight program gave impetus to an American space program that met President John F. Kennedy's challenge to the nation of *"achieving the goal, before this decade is out, of landing a man on the moon and returning him safely to the Earth."*

Today we face the need for an ever-more-effective Community leadership and the constantly changing requirements of those in government who rely on intelligence. If the nation is to meet the challenge of a truly effective national intelligence capability—one able to support the global war on terror, to detect programs to develop and employ WMD, and to provide our leaders with the means to address other sustained national security concerns and interests—it must do so with the resolve and approach exemplified by those who won World War II, took America to the moon, won the Cold War, and helped us meet other critical national challenges.

Nothing less will suffice. Nonetheless, something less is what we might choose.

As always, there are at least two approaches to meeting serious challenges. One approach, exemplified by the incremental steps we have taken in recent years, represents a checklist of things done to address the concerns of Congress, the 9/11 Commission, and other stakeholders. This approach identifies specific weaknesses (for example, failure to connect the dots and lack of system interoperability), mitigates incrementally those weaknesses, and builds management structures that avoid their reoccurrence. In effect, this approach is very much like going to the moon a foot at a time, and measuring each day how much farther we are from the ground. It constantly compares our progress to the point from which we started.

The other approach reflects more clearly the nation's successful efforts to make truly significant progress in the face of difficult odds and stringent timelines. This approach provides first an image of what and where we want to be and measures each day by how much closer we are to our goal, rather than by how far we've ventured from our starting place. *It recognizes that our destination is more important than our place of departure,* and it compels us to measure our progress accordingly. This approach was fundamental to our early overhead reconnaissance efforts.

However we proceed, building a national intelligence workforce (or National Intelligence Service) cannot be done merely by harmonizing grade structures and arranging more frequent interagency rotations. In a similar light, a national intelligence information system will not emerge through the development and imposition on an interagency basis of common data and meta-data standards. Both outcomes require a top-down vision and commitment as well as the authority appropriate to their accomplishment.

In the end, this paper describes some aspects of the objective vision, to which the Intelligence Committee believes the nation must build, rather than describing incremental improvements that take us step by step away from today's situation.

3. Scope of the Challenge—A Nation's Expectations in a New National Security Environment

As citizens of the world's most powerful and influential nation, Americans rightly expect that civilian and military decision makers should have at their disposal the most relevant and accurate intelligence available to any nation—intelligence that is always timely to whatever decisions are faced by our nation's leadership. American national security interests range from preempting short-term efforts from terrorists, to helping position us to meet international economic competition. National strategies and investments in defense and scientific research, homeland security decisions, and diplomatic and international economic policy rely on the best intelligence the Intelligence Community can provide. Although national attention was riveted by the attacks of 9/11, Americans would not take lightly lapses in our ability to deal effectively with other national challenges. For example, China's economy continues to experience the highest growth rate of any major economy; China's GDP is now just more than half of that of the United States. Preserving and extending American prosperity depends on understanding the competition and opportunities presented by nations such as China and on helping government executives and lawmakers determine how best to focus economic and fiscal policy in support of U.S. economic interests and advantages.

At the same time, China's economic power provides it with new possibilities for military development. While Chinese military technology does not overall represent a challenge to the West, the Chinese are moving to deploy nuclear submarines; standoff/cruise missiles; laser rangefinders and computerized fire controls for tanks; more advanced aircraft; the foundations of a modern C4I infrastructure; and new classes of weapons. China is reported to be working on aircraft carrier design (and has purchased an ex-Soviet carrier). Chinese scientists and technologists have demonstrated recently the ability to place an astronaut in orbit, a feat that requires top-class prowess in a wide range of technologies and a considerable supporting infrastructure. One can expect China's demonstrated capability to mass-produce complex consumer electronics to be a valuable resource base for modernizing its military force.

As China's economic and military power grows, so too will its international posture and prerogatives. Our prerogatives conversely may be constrained as China becomes more independent and capable of influencing the course of international affairs. As American international indebtedness increases (the U.S. borrows approximately $540 billion each year from foreign sources), we may face additional constraints. Americans are entitled to know that their leaders understand this situation, and that America's prerogatives, influence, and well-being will not be overwhelmed by surprise or be compromised over time.

WMD developments by other nations may occur slowly, but they can be dramatic in their effects on the international situation and in American regional interests. Pakistan and India have both demonstrated nuclear weapons technologies, and it is reasonable to expect that both nations have weaponized that technology. Iran, North Korea, and others have demonstrated a sustained commitment to acquiring nuclear technologies pertinent to military applications. Nations that embark on regional "adventures" (such as Argentina's effort in the Falklands/Malvinas) may find themselves overwhelmed

by their own miscalculations. Such nations may seek rapid redress in their fortunes through the most extreme measures, perhaps including nuclear weapons. Again, Americans are entitled to the assurance that their government understands these developments clearly and that, when leaders take action (economic, political, diplomatic, or military) to protect our interests, those leaders are as well informed as possible by superb intelligence.

Nonetheless, Americans have not always had the benefit of the best intelligence possible. Pearl Harbor represents an inability to recognize threat information for what it was, to disseminate that information to decision makers who needed it, to know that intelligence was integrated sufficiently well into those decision makers' concepts of operations, and to ensure it was used effectively. America paid dearly for that failure. India's nuclear tests in 1998 surprised American national security decision makers. Those tests led to a swift series of countertests by Pakistan, bringing a passionate regional nuclear arms race to the open. Without sufficient warning, American diplomacy (and other tools) could do little to discourage either the Indian or Pakistani tests. America has been living ever since with the results, a situation in which four contiguous nations (Pakistan, India, China, and Russia) have nuclear weapons (or weapons technology), in which three (Pakistan-India and India-China) have difficult relations, and in which two (Pakistan and India) have come to blows both frequently and recently.

Of course, the events of 9/11 also represent a situation in which a lack of clear warning constrained America's ability to prevent a tragedy. Americans have had to live since 9/11 in a changed, and far more difficult, world. Even as we ponder the absence of a major attack on American soil since the fateful events of 2001, we must accept the possibility that those events might have represented an ever more ambitious plan that did not come to fruition, and that such a plan—years in the making—may yet result in an even more devastating effort by our nation's enemies to damage and isolate the United States. If true, the "failure of imagination," of which the 9/11 Commission wrote, is a danger we may not yet have overcome in full.

We cannot take comfort in the fact that we have a capability that is optimized for the last war or crisis; we must have the foresight and flexibility to be prepared for the unknown. Americans expect and are entitled to a national intelligence capability that creates opportunities, rather than one that merely helps decision makers accommodate the nation to more difficult circumstances.

4. Positioning Intelligence for the Future—Intelligence Concepts and People

4.1 Concept and Doctrine Development

Building a national intelligence capability—creating an extended enterprise for intelligence that starts with a vision of how effective, timely, accurate, and comprehensive intelligence must be—needs to be accompanied by a discussion of future intelligence concepts. Perhaps more important is the consideration of a permanent capacity to examine and validate intelligence concepts and the concepts by which intelligence is organic, on a regular basis, to the military, political, diplomatic, economic, and other activities it supports.

Precedent exists for an approach of this sort. The armed services, through structures such as the Army's Training and Doctrine Command, the U.S. Army Center for Land Warfare, the Center for Naval Analysis, and the Air Force Doctrine Center, look constantly at new operational concepts—in

some cases translating them into doctrine and training requirements. At a higher level, the DOD Office of Force Transformation is seeking to further the Revolution in Military Affairs, and it encourages powerful examination of new ways to organize and fight. The Joint Transformation Roadmap represents tangible expression of the need to put forth new concepts of operations. Consider how the roadmap describes joint intelligence, surveillance, and reconnaissance (JISR) as organic to operations:

> *"Dynamic JISR will deliver a joint "all ISR" capability that reflects doctrine, tactics, techniques and procedures, training, materiel, and leadership and education elements. This concept will enhance overall warfighting battlespace situational awareness by delivering powerful ISR visualization, optimization and operations-intelligence synchronization capabilities to the ISR battle manager and collection manager. The ISR battle manager and collection manager use dynamic JISR capabilities to update the common operational picture, thereby providing a more accurate and complete operations/intelligence view of the battlespace."*

The roadmap represents an example of both the end-state and process of future concept of operations development as well as highlights the manner in which intelligence can support future operations.

Continuous examination of future concepts and doctrines that inform our investments and behavior represents the genius of American industrial organization. Indeed, the ability to build new concepts and doctrines revolutionized America's World War II armed forces and industrial capabilities. It allows America to lead the world in building new economic structures and in stimulating development and deployment worldwide of advanced information technologies and the products and services that rely on them. American intelligence needs—in fact, it requires—a similar strategic perspective, one that questions constantly our operational concepts and doctrines, assessments, and estimates processes and one that looks at how we are organized, what we do, and how we do it. Like any other serious aspect of America's national life, the art of intelligence cannot remain static. An Intelligence Concepts and Doctrine Office, coupled to intelligence training and professional education, should report to the new National Intelligence Director, much as the Office of Force Transformation supports the Secretary of Defense.

4.2 Building and Developing an Excellent National Intelligence Workforce

Hand-in-hand with the development of new operational concepts and doctrine is the need to develop a national intelligence workforce. Today's workforce represents crafts specific to discrete functional disciplines (such as collection, processing, exploitation, analysis, and reporting) and collection means (such as HUMINT, SIGINT, MASINT, IMINT, OSINT). National intelligence problems, however, are rarely so defined. For example, international terrorism represents a global dispersion of resources and influence, and foreign WMD programs encompass large and complex infrastructures. America needs a workforce equipped with unified standards of excellence, trained to understand the entirety of the intelligence product they produce. This is not to say that specialization is not required or desirable. Intelligence will continue to need specialized mathematicians, engineers, analysts, regional experts, translators, and others.

However, a workforce in which standards of performance differ, as do requirements for professional certification, impedes adoption of concepts and doctrine developed around the need to understand

targets and problems rather than the need to master crafts. In addition, a national intelligence service shifts behavioral incentives away from crafts and today's individual infrastructures toward a more unified Community. In doing so, it reflects lessons learned in the defense community about the need to ensure that potential flag officers serve in joint assignments, mastering the demands of joint and combined operations by virtue of their professional development and experience. Again, as the nation moves away from analytic infrastructures specific to individual collection means (for example HUMINT and SIGINT) to competitive centers of analysis—each of which has access to all of the data seen by other centers—we will need a workforce capable of dealing in the entirety of intelligence rather than in the nuances a specific means of collection only.

As a result, the nation would benefit from a national intelligence service such as that described by the 9/11 Commission report. Whether or not elements of that service are assigned to specific departments and agencies, career development within that service should be subject to consistent training, levels of achievement and recognition, promotion, assignment, incentives, and professional accreditation. A national intelligence service represents the most reliable means by which a national cadre of intelligence professionals will build Community-wide *esprit de corps*, associating with each other and the larger intelligence mission rather than individual organizational components.

We cannot overemphasize the importance of high quality and consistent training of members of a national intelligence service. While technical specialties within organizational components may benefit from training conducted by those components, training related to intelligence concepts, doctrine, analysis, research, estimates, customer relations, general management, and executive management should be conducted within a training context managed as a Community-wide asset, subject to consistent levels of quality in curriculum development, execution, and expected results.

4.3 Behavioral Incentives

Even as the debate continues regarding the extent to which one organizational model or another is pertinent to rebuilding our national intelligence capability, the principle of giving incentives to reinforce the behavior the Community wants to encourage can hardly be denied. The Goldwater-Nichols DOD Reorganization Act of 1986 (Goldwater-Nichols) made clear the need for joint training and experience as prerequisites for promotion to general officer. Giving the services—and their officers—an incentive for joint behavior has amplified the effectiveness of our armed forces, accelerating inter-service understanding of capabilities and concepts, spurring the development of joint warfighting doctrine, and substantially enhancing the ability of our services to gain battlefield superiority. Indeed, the asymmetrical advantages enjoyed by U.S. armed forces are in part related to joint warfighting.

National intelligence can do no less. If we demand the emergence of a true national intelligence capability and if we anticipate the development of a national intelligence cadre, then we need to provide career incentives to national intelligence professionals to serve throughout the Intelligence Community, to demonstrate leadership outside of their own specialties, and to exhibit an understand of intelligence as a unified discipline. To that point, promotion to the rank of senior intelligence executive should be contingent upon successful completion of national intelligence assignments at a variety of levels, demonstrating broad competence in addition to mastery of discrete intelligence specialties.

5. Integrated Intelligence Capabilities—New Structures

The development of a truly integrated national Intelligence Community requires the promotion of intelligence as an integrated discipline. Today's National Intelligence Council (NIC) is focused principally on the fusion of analysis. Still to be addressed are issues relating to combined collection and analytic strategies that encompass a wide variety of today's intelligence disciplines (such as HUMINT, SIGINT, IMINT, MASINT, and OSINT) and that provide intelligence consumers with smooth access to intelligence capabilities without requiring those consumers to specifically task each discipline. Such an approach would give consumers, many of whom have a sophisticated understanding of both intelligence and the subjects in which they are interested, a window into the collection and analytic strategies being employed on their behalf. Such an approach is consistent with the provision of information services in the larger e-government and American information services environments. Subject to effective security mechanisms, the Intelligence Community should adopt such an approach.

To a certain extent, the Community has already experimented with this approach in the Intelligence Community Multi-Int Acquisition Program (ICMAP). Most efforts, however, have been *ad hoc* bilateral endeavors between agencies. Impeding progress in this domain has been the lack of adequate authority and resources throughout the Community for an integrated intelligence discipline. In contrast, Intelligence Community overseers have contended with individual agencies to gain modest resource commitments, and the commitments are made at the expense of ongoing programs within these agencies. Integrated intelligence, therefore, lies at the mercy of existing intelligence disciplines, concepts, and structures. To the extent possible, authority for integrated intelligence should start with the National Intelligence Director and be expressed as:

- A component of the new intelligence concepts and doctrine developed within the Intelligence Concepts and Doctrine Office (described earlier); and
- A formal mission requirement and architectural component intrinsic to the design of intelligence systems acquired by a Director of Technology, Architecture, Engineering, and Acquisition (described later).

In effect, the National Intelligence Director should ensure that effective program management exists for integrated intelligence.

The following sections offer additional discussion on structural ways to achieve integration.

5.1 Unified Collection

The challenge of intelligence collection is, *inter alia*, characterized by the statement: "Know something about everything all of the time; know everything about something when you need to know it." Policy makers cannot predict what they need to know and when they will need to know it. But they rely on intelligence to provide them with relevant information in the right amount of detail at the right time. This is the challenge the Intelligence Community has attempted to meet since its inception: predict policy makers' information needs, collect and analyze appropriate data, and provide answers on time. This highly entrenched tradition argues that any reforms that remove policy makers further from

routine and daily interaction with their intelligence advisers are misguided. Any centralized planning, programming, and budgeting must be supported by decentralized execution of those plans and budgets.

While it is true that the Cold War molded the Community's structure and shaped its methods for collecting intelligence, the Cold War is not the sole basis for why we are where we are today. Other factors have contributed significantly. Intelligence collection disciplines traditionally have been esoteric. The structure of the Intelligence Community reflects that esotericism. Careers of many intelligence professionals have been built on achieving a comprehensive understanding of the strengths and weaknesses of a wide variety of collection systems, their relationships to each other, and their capabilities to contribute to solving an intelligence problem. Moreover, each of the traditional collection disciplines (IMINT, SIGINT, HUMINT) and the newer disciplines such as MASINT often involves complex systems that rely on arcane procedural rules, some of which reside within highly secretive security compartments.

Moreover, legal constraints that apply to one collection discipline and not to another add an additional dimension to achieving a comprehensive understanding of how to collect the right intelligence with the right combination of capabilities. In their totality, these dimensions are not easy to understand. Many of the so-called stovepipes are based on the unique nature by which intelligence is collected within the different collection disciplines. Professionals can spend an entire career trying to achieve the comprehensive knowledge required to exploit intelligence collection capabilities fully.

We who advocate intelligence reform hope to achieve an integration of the collection (and other aspects of the intelligence cycle) in a way that exploits (in the short term) individual system strengths and overcomes (in time) gaps by achieving synergy among all systems. Key to achieving these goals are collection management (and mission management) capabilities designed in a manner consistent with an integrated intelligence concept. Such systems should help develop collection (and analytic) strategies that cross today's intelligence disciplines. New systems should include interfaces to common collection and mission management systems. The Director of Technology, Architecture, Engineering, and Acquisition should promulgate common interface standards for both management systems and the mission systems they manage as system requirements.

5.2 Common and Competitive Analysis

The national discussion of intelligence capabilities often focuses on the need for competitive analysis, (that is products from competing analytic centers). This need is used in some cases to justify the existing structure of the Intelligence Community, or at least the separate management of individual intelligence components.

The current situation, however, lacks three components necessary for truly effective, deep, responsive, and useful analysis. Indeed, the creation of an effective National Counterterrorism Center[2] as mandated by the President will be made more difficult until these components are addressed. First, the current structure restricts access to data specific to individual intelligence disciplines. The Intelligence Committee understands clearly that much data (for example, raw SIGINT data that is unprocessed) may not be pertinent for analysis. Still, competing analysis based on different data sets makes difficult the comparison of analytic results. Much as other professional disciplines (such as medicine and

[2] Executive Order - National Counterterrorism Center August 27 2004

science) rely on peer review using common data and reproducible conditions, truly competitive analysis must rely on as much commonality of data, information, and knowledge regarding targets as the Community can contrive. To that extent, knowledge bases and data that can be shared as far into the supply chain as possible should be made available across the Community. Personal key identification (PKI) and other technologies that allow for automated security access management, federated query, and enterprise data management should be employed to enable truly competitive products in which analysts and consumers can question each other's assumptions and conclusions.

Second, the current, independent analytic structure makes a 360-degree analysis (which includes every aspect of the topics and targets we wish to understand) more challenging than is necessary. A common analytic infrastructure would allow better social network analysis and general connectivity among data collected by a wide variety of means (and from many sources) and collected in accordance with the widest range of interests and requirements. Given today's intelligence challenges (for example WMD and dispersed international terrorism), analysts need to approach every target from the widest possible variety of aspects, to seek intra- and inter-target relationships, and to view each target as a conceptual whole instead of as a series of discrete issues and snapshots.

Third, the current analytic structure impedes mutual awareness among elements of the analytic community. Even as analysts learn to see each target as a whole, they need to see the Intelligence Community itself as a whole. More specifically, each analyst should know who else is working on a problem of interest, on what aspect each person is working, who has what information, and what insights each person can offer.

While a number of models exist for achieving these ends, the deployment of a common analytic infrastructure (with appropriate technologies) is a vital step in addressing the need for truly integrated and competitive analysis, particularly against complex, dynamic, and transnational targets. Equipped with such an infrastructure, the Community could create a new analytic corps, one capable of stronger multi-disciplinary analysis and prepared to help revitalize our ability to provide decision makers intelligence reflecting sustained research. Equally important, however, is the need to ensure that the Community has access to appropriately manned and provisioned competitive analytical entities, each having the same data available (consistent with the principles of peer review used in most professions).

5.3 An Organic Capability for Self Improvement

As indicated previously, America's industrial leadership is based in large part on its national ability to analyze continuously how we act and how we are organized, changing our functions and organizations as necessary. Indeed, the disciplines of industrial organization, operations research, and systems analysis that emerged during World War II aided both our World War II and Cold War victories.

The National Intelligence Director should gain for the revitalized Community the benefits of America's unique ability to plan, organize, and operate dynamically. To that end, the Director should put in place a national center for intelligence process design, similar, perhaps to DOD's Net Assessment organization, that would function at a level higher than the concepts and doctrine component described previously. This center would study intelligence processes, operations, and structures, recommending to the National Intelligence Director high-level insights into future

Community enhancements. Such insights might be used by the Director to help craft multi-year program development and budget guidance used to shape Community resources and capabilities.

5.4 International Intelligence Relationships

The integration of national intelligence described in this paper (and other by commentators) reflects an extended enterprise approach that links a wide variety of processes and capabilities. The United States, as the senior partner in a number of bilateral and collective security arrangements, should exercise additional leadership in the development of complementary intelligence capabilities among key allies. To the extent possible, common architectural standards, information models, data (and meta-data) standards, as well as common processes should be used to build international intelligence capabilities that make more robust our own capacity to understand the diverse threat environment our world faces. Asymmetry that makes it difficult for allies to adopt U.S. technical standards and technologies impedes our ability to gain access to intelligence these allies can provide. Many of the information technologies on which the U.S. Intelligence Community relies are based on commercial technology platforms and approaches. The U.S. should make it a top priority to help allies deploy these technologies in a manner more likely to interoperate with U.S. capabilities. PKI and other enterprise data management technologies can be used to manage access and to protect sources and methods.

6. Industry Partnership and a National Intelligence Architecture

6.1 Architecture, Engineering, and Acquisition Authority

Although discussion is underway regarding the extent to which a new National Intelligence Director would have budgetary authority, more focus is needed on the question of how that authority would benefit from the creation of a stronger national intelligence capability.

The complexity of the intelligence challenge—and the need for intelligence to support more organically its customers government-wide—will require increasingly advanced capabilities. Many of these capabilities are technology-based. Other capabilities may be more specific to discrete disciplines (aspects of HUMINT, for example). However, the totality of these capabilities should be understood and managed within the context of a national intelligence investment.

The AFCEA Intelligence Committee's previous white paper described certain technology-based opportunities available today for the development of a stronger, more integrated Intelligence Community. Those opportunities, however, rest on assumptions regarding the extent to which information systems standards, interfaces, communications protocols, bandwidth capacities, and other aspects of technical performance can be made consistent across these aspects of the intelligence that employ them. Although mechanisms exist today to harmonize requirements (and resulting capabilities), these mechanisms lack the strength necessary to build an integrated national intelligence investment. The Joint Requirements Oversight Council and Mission Requirements Board provide some impetus to the integration of requirements, but only to the extent that general requirements are met and do not overlap. CIO-like efforts in the Intelligence Community focus on data and meta-data standards. However, more is needed if systems are to work together, making integrated collection and mission management possible and analysis in which competitive analytic centers have access to the same data, allowing real peer review. In addition, integration of intelligence with operations, as described in the

Joint Transformation Roadmap, goes beyond mere interoperability. In this context, intelligence systems become organized with the operational systems with which they work.

Efforts have taken place (and continue) to build a more integrated set of intelligence capabilities. The Unified Cryptologic Architecture describes a set of standards and interfaces for cryptology. The Navy has developed a C4ISR-compliant architecture. The Army's Future Combat System will rely heavily on the integration of ISR capabilities to compensate, in part, for giving up the protection of heavy armor characteristic of most current combat platforms. Many expect intelligence systems to work with the Global Information Grid. Less emphasis has been given to the integration of intelligence systems with non-DOD customer systems. That emphasis is needed.

Overall, the process of building a national intelligence investment, representing integrated requirements, standards, interfaces, services, and systems remains fragmented. Some systems are compliant with the Defense Information Infrastructure and Common Operating Environment; others are not, and no single authority to adjudicate compliance has emerged. The Clinger-Cohen Act requires departments and agencies to appoint a CIO, presumably with adequate authority. This requirement, like others aimed at making the most of our precious national investment, is met sporadically.

Given the urgency of a stronger national intelligence capability, consideration should be given to a Community-wide Director of Technology, Architecture, Engineering, and Acquisition, equipped with the authority to approve technology standards, oversee development of intelligence systems, and approve inputs prior to submission to the Congressional Budget Justification Book and the Presidential Objective Memorandum. Whether or not a CIO advises this director or is encompassed within this director's organization, the director should ensure that systems reflect integrated requirements and capabilities, moving the nation toward a stronger intelligence capability that makes the most of the available and emerging technologies. Such a director would be in a position to ask hard questions relating to the segmentation of today's capabilities based on practice, tradition, and craft. In contrast, this director could ensure—through integrated budget submission—that new capabilities really do work together.

Some of these authorities do exist today, but they are handled on a fragmented basis. For example, the Intelligence Community has both a CIO and a senior acquisition executive (SAE). The Intelligence Community responds as well to the Under Secretary of Defense for Intelligence (USDI) and the Under Secretary of Defense for Acquisition, Technology, and Logistics (USDAT&L). In fact, the Office of the Secretary of Defense holds milestone decision authority for parts of the Intelligence Community. Budget submissions flow through a variety of channels, none of which is currently equipped to take a top-down, standards-based system-of-system look at the capabilities for which funding is requested. Resulting far too easily are gaps that must be filled and overlaps on which resources might be wasted.

6.2 Industrial Partnership and the Acquisition Corps

Industry's ability to support a revitalized Intelligence Community is constrained by inconsistent acquisition approaches. The lack of a unified acquisition philosophy impedes both the development of integrated and interoperable systems and of capabilities developed to consistent levels of quality and reliability. It is often difficult to understand the selection of a contract type and acquisition approach

for specific procurements. Different Community components give varying emphasis to cost, technical adequacy, architecture, engineering, mission understanding, or program management.

The application of a more consistent approach to acquisition requires a revitalized Intelligence Community acquisition and program management corps. Such a corps should operate from a consistent acquisition strategy and reflect the benefits of common acquisition and program management training. This corps would be both more consistent and more discerning in its relationship with industry. It would transfer knowledge smoothly throughout the Community regarding sound acquisition and program management practices. It would strengthen the need to integrate both the capabilities of systems the Community plans to acquire and the schedules by which acquisition takes place. Such an approach would give industry a clearer view of the capabilities the Community requires, enabling industry to invest in the R&D and business development resources necessary to couple efficiently to the Community's plans. Finally, it would give industry the opportunity to develop and present technologies to the Community that can address a wide variety of needs, reducing the likelihood that individual Community components would acquire competing technologies for similar (or the same) requirements.

6.3 Industrial Partnership and Security

Industry's ability to support a revitalized Intelligence Community is also constrained by a lack of cleared people and inconsistent security regimes. The Community's industrial partners need the ability to deploy their professional resources more flexibly for the development of a new generation of technical capabilities and to provide vital staff augmentation. The lack of a unified security administration regime makes this deployment difficult, even as it reduces the size of the pool of cleared professional resources. Companies (and their employees) are faced with the need to manage clearances and accesses across a range of security structures. Such an approach increases costs, slows deployment, and can drive skilled people to other opportunities that employ their skills, particularly when the national economy is strong. In fact, the current security and access approach can impede even the flexible deployment of government professionals. One approach that could greatly ease this problem for government and industry alike would be for government agencies to continue to hold the clearances for all personnel who leave (retire or resign) and seek private sector employment that requires clearances and accesses.

The National Intelligence Director has an important opportunity to help overcome these impediments to a stronger, more integrated national intelligence capability. In addition to the approach described above, other milestones in capturing this opportunity include:

- Compulsory common application of industrial security policy; adoption of the recommendations put forward by a variety of industry groups, including the Professional Services Council (PSC), the Security Affairs Support Association (SASA), the Contract Services Association (CSA), the Northern Virginia Technology Council (NVTC), and AFCEA (collectively, the Coalition) to address the clearance logjam; and
- establishment of common clearance and access regimes (including security investigations and adjudication); and creation of a common intelligence security corps spanning the new Community.

7. Accelerating Progress

In preparing this paper, the Intelligence Committee researched the various studies and commissions that have suggested ways to strengthen national intelligence. These commissions (for example, Brown/Aspin, Scowcroft, Boren/McCurdey, IC21, and 9/11) point to a number of potential enhancements to national intelligence. Common themes include combined collection, common architecture, improved coordination, less cumbersome information sharing, and others. Recent executive orders and a variety of proposed bills (from both the House and Senate) reinforce the public sense of urgency associated with rebuilding our nation's Intelligence Community.

The events of 9/11 and subsequent inquiries make possible the perception that national intelligence has not improved in recent years. The Committee does not share this view. On the contrary, considerable progress has been made and is ongoing. Where common operational concepts have been developed (pairing agencies such as the NRO with the NGA, for example), elements of a common architecture have emerged. Planning for the Cryptologic Mission Management System extends beyond NSA. Meetings by lead analysts held each day have made interagency (and inter-disciplinary) collaboration more routine. Our ability to collect and analyze information and integrate intelligence into operations made possible the capture of Saddam Hussein and has been key to diminishing the leadership ranks of the nation's terrorist adversaries. Intelligence and law enforcement senior executives are working each day to improve information sharing across the intelligence/law enforcement divide while respecting constitutional principles and sustaining constitutional and statutory limits. More and more intelligence systems share common technical standards, and many are adopting technical standards that improve interoperability with defense capabilities. Support to warfighters has never been stronger. Experiments such as Quantum Leap are exploring new ways of disseminating vital information swiftly to combatants, coupling defense intelligence to emerging concepts of network centric warfare.

This progress must be sustained if it is to be generalized across the Intelligence Community. Although the Community's existing CIO's and senior acquisition executives have, in principle, some authority to cause creation of a system of systems (and capabilities) based on consistent technical standards and technologies, they lack the resources to ensure their application. They are also not included/accepted into the mainstream of the traditional intelligence process. More to the point, the integration of the Intelligence Community remains impeded by the lack of a unified operational concept—sponsored from the top. Such a unified operational concept—coupled with the architecture, engineering, and acquisition plans expected to enable that concept and staffed with acquisition and program management professionals equipped with common methodologies—would give teeth to principles the Community has accepted, but not employed. Accompanied and enabled by mechanisms to ensure that budget submissions conform to an integrated concept, integrated programs, and integrated capabilities, the National Intelligence Director would be better equipped to build the Intelligence Community the nation requires.

8. Summary: Government and Industry--Rebuilding a National Treasure

Consistent with the preservation of our constitutional principles, nothing is more important than a national intelligence capability that provides decision makers with intelligence pertinent to vital decisions ranging from tactical operations to strategic, national investments. The questions decision makers face are complex. Few of them are constrained to answers that can be extracted from a specific

intelligence discipline or craft. Only an Intelligence Community that integrates these disciplines as much as possible, building common mission management systems for integrated collection, processing, exploitation, analysis, production, and customer support, can help answer such questions. New operational concepts, fusing these disciplines and crafts, are essential to this integration. A national intelligence workforce, subject to a unified security regime and equipped with multi-disciplinary career development, would create new, powerful teams capable of analyzing complex intelligence challenges throughout their entire circumference. Systems acquired by a new, common acquisition and program management work force, built to complementary requirements, using a common architecture, would enable these teams to function with unprecedented effectiveness. Budget authority, expressed as the ability to ensure that program and system acquisition reflect integrated requirements, technologies, and capabilities, would make possible the collaborative information system of systems the Community needs and for which many commentators and lawmakers, as well as the President[3], have called. Such an approach, in turn, would give industry a stronger partner with which to work, make industry's capabilities more transparent to the Community, and allow industry the flexibility to deploy its best resources to the Community's most urgent problems.

The journey to building a new national Intelligence Community is underway. The nation expects us to make this journey. Our citizens are justified in expecting that we will.

[3] Executive Order – Strengthening the Sharing of Terrorism Information to Protect Americans, August 27, 2004.