National Security and Horizontal Integration

Introduction

This paper: a) describes the integration of intelligence based on the work already undertaken by the leadership of the Intelligence Community; b) identifies opportunities to achieve that integration; and c) provides recommendations to national security decision and policy makers relevant to those opportunities. The Armed Forces Communications and Electronics Association (AFCEA) Intelligence Committee offers this paper based on a desire to strengthen the effectiveness of the Government/Industry partnership in further development of intelligence capabilities at all levels. Thus, the overall focus of this paper is on steps that can be taken now to leverage the Intelligence Community gains from industry more effectively.

Integration – The Need and the Opportunity

The attacks on the United States of September 11, 2001, and subsequent developments in the national security situation, highlight the need for an Intelligence Community that provides more effective threat warning, that gives better help to warfighters, and that better supports national security decision-making. Just as important is the need to provide swift and decisive support to war fighters who must act within the decision-and-action loops of adversaries. These needs however pre-date the events of 9/11 and, despite significant progress in strengthening national intelligence capabilities, remain important challenges.

Overall, the structure of today's Intelligence Community, including regulatory, organizational, budget, infrastructure, and other components, reflects the development of a community based on intelligence disciplines that have varied traditionally in their operational concepts, technologies, applications, and (in some cases) customer communities. Human Intelligence (HUMINT), for example, at the national level serves national intelligence requirements. Within the armed services, however, HUMINT often serves theater and tactical operational needs. Specific HUMINT infrastructures exist to support these needs and their associated customers. Imagery Intelligence (IMINT) and Signals Intelligence (SIGINT) have served both national and tactical customers, although the traditional focus of IMINT has been largely national. SIGINT, in contrast, has developed infrastructures dedicated to specific national systems and targets as well

as other infrastructures that support the war fighter more directly. Finally, Measurement and Signature Intelligence (MASINT) is emerging as a set of specific capabilities within individual components of the Intelligence Community. As intelligence problems have become both more complex and more diffuse, the Community's customers are becoming increasingly familiar with MASINT's capabilities and products.

Two overarching changes in the environment surrounding intelligence have increased the need for a more integrated Intelligence Community while creating powerful opportunities for achieving that integration.

First, the mission set supported by intelligence is less likely than before to be characterized by sharp divisions between customers of national and tactical, diplomatic, political, economic, and military intelligence. Each of these components is strongly related to the others. For example, a complete picture of another nation's WMD program must convey not only that nation's diplomatic and economic relations with nations that may be supplying the technology (or to which it may be supplying technology), but also the electronic intelligence (ELINT) regarding specific systems.

Second, information technology offers the opportunity for a closer, more organic national intelligence capability—one characterized by a unified "value chain," rather than the individual infrastructures (and value chains) associated traditionally with each intelligence discipline. Today, contemporary information technology enables large enterprises to manage disparate infrastructures uniformly in support of a wide range of customers and products.

Senior Intelligence Community officials recognize the need for a strengthened, more integrated Intelligence Community. Under the chairmanship of the Under Secretary of Defense for Intelligence (USDI), a Horizontal Integration Senior Steering Group (HISSG) has undertaken an effort to define horizontal integration and, by extension, intelligence integration. That effort has led to a focus on *"processes and capabilities to acquire, synchronize, correlate, and deliver National Security Community data with responsiveness to ensure success across all policy and operational missions."* The vision statement adopted by the Steering Group makes clear the imperative to focus on the *"mission needs of policy-makers and operators, not on the providers of information or intelligence."*

The steering group's view encompasses the need to move from data ownership (implying ownership by a specific intelligence discipline or infrastructure) to data usability (viewed explicitly from the perspective of the needs of policy-makers and operators). The vision extends itself to policy and regulatory issues, calling for the conformance of *"legal, security, and policy guidance"* to a *"consumer-centric construct."* Finally, the vision recognizes implicitly the opportunities for a more unified approach to the management of the intelligence value chain, calling for *"end-to-end management and integration of information and intelligence functions,"* including *"requirements, tasking, collection, operations, correlating, tagging, exploiting, archiving, fusing and analyzing"* as well as *"communications, infrastructure, policies and procedures."*

This paper focuses on ways to achieve the integration that the Steering Group and others are seeking. As a result, it makes no further effort to define "integration," relying instead on the emphasis already placed on more integration among intelligence functions; more unified management of those functions; conformance of legal, policy, and regulatory guidance to the needs of integration; and a more integrated intelligence infrastructure.

A DCI-led offsite in November 2003 reached similar conclusions. That offsite called for *"expeditious sharing of collected data and full information transparency enabled by tagging data at or as close to the source of data as possible."* It recognized the need, across the Community, for *"commercial-sector models – Enterprise Management, Enterprise Portfolio Management, and Enterprise Architectures"* as well as *"commercially available…tools* [that] *can help an analyst discern and understand obscure linkages between individuals, activities, and methods of operation…"* Finally, the offsite called for Community-wide ***"tagging standards allow the use of sophisticated "analytic discovery" tools to further refine both queries and answers."***

The observations offered by the HISSG and the DCI's offsite describe a Community-wide approach to analytic standards and tools, engineering, and architecture. These elements serve a larger vision of an integrated Intelligence Community in which *intelligence itself* is an integrated discipline and the value chain from which intelligence consumers (decision-makers and operators) derive intelligence is integrated as well.

Industry and the nation's technology (and information technology) base are prepared to support this vision. U.S. industry has pioneered the use of integrated value chains. Larger enterprises—and in some cases entire industries—have built data and tagging standards. Industries ranging from automobile parts manufacturer and supply (using an industry-wide business-to-business datamart) to nationwide retailers (adopting a national radio frequency identification standard to manage inventory) are building and implementing enterprise-wide systems. Such systems give consumers highly customized products while gaining the efficiencies that come from common, enterprise-level platforms and supply chains.

Two basic approaches could help the Community achieve this vision. These approaches also roughly bound the range of implementation concepts available to the Community.

In the first approach, the Community defines systems that can be implemented by individual agencies, within their specific disciplines, infrastructures, and programs. The approach relies on each agency's own engineering and acquisition organizations and practices.

In the second approach, the Community sponsors an enterprise architecture, design, and acquisition approach. The Community would treat the acquisition of integrating capabilities and technologies as part of a unified discipline and the unified infrastructure for which the HISSG has called.

Both of these approaches are in use today. The first approach is exemplified by the Unified Cryptologic Architecture (UCA) effort, led by the Director, NSA, in his role as cryptologic functional lead within the Expanded Corporate Management Review Group (ECMRG). The UCA Office (UCAO) is a Community organization, supported by NSA and managed within NSA's System Engineering organization. As such, architecture and planning efforts for Community-wide implementation are in a manner consistent with NSA's own system engineering efforts. However, other components of the nation's cryptologic system conduct system engineering and development more in accord with individual mission requirements. The extent to which these components adhere to UCAO principals (and the architectural requirements that support the UCA) is left largely to the discretion of individual program managers operating within their own disciplines and infrastructures. To the extent necessary to achieve common functionality or data sharing, program managers negotiate bilateral agreements for inter-system connectivity or joint system development. This approach has led to a number of useful capabilities, but it has not led to an integrated plan or program for a Community-wide cryptologic capability with discrete funding and management responsibility.

The second approach, in which design, engineering, and acquisition of Community-wide capability is being attempted within the existing structure of the Intelligence Community, is exemplified by the Intelligence Community Multi-Intelligence Acquisition Program, or IC-MAP. This program has direct oversight by the Assistant Director of Central Intelligence for Collection. Acquisition management is currently being performed by one of the Community's constituent agencies. IC-MAP's focus is on central and consistent management of intelligence requirements, giving national security decision-makers and operators "one-stop shopping" for their intelligence needs. This focus recognizes that intelligence consumers are busy, that their needs change, and that the burden of managing their own requirements through the various infrastructures and value chains comprising the Intelligence Community should be lifted from their shoulders. In this regard, IC-MAP is attempting to follow the lead set by the private sector, in which consumers can gain customized products from vast enterprises using relatively simple portals. The management of internal infrastructures and value chains to provide these products is largely not visible to the consumer.

This approach has met with challenges. While the IC-MAP program office has gained the participation of Intelligence Community agencies (through its Business and Policy Committee), support for the program has been inconsistent. Each agency supports its participation in IC-MAP within the priorities considered for each agency's mission. Changes to each agency's programs and acquisition plans to accommodate IC-MAP are voluntary. The Community has found difficult the establishment of a supra-agency planning and budget process in which IC-MAP requirements are met consistently throughout the Community and in which individual programs are modulated to support IC-MAP architecture, schedules, and milestones.

Over time, it may be useful to consider a model in which a single intelligence discipline, supported by a single intelligence infrastructure, supports national security decision-makers and operators. Such a model, however, would require significant structural changes in the Community, as well changes to supporting law and regulation. While a Community integrated

completely along horizontal and vertical lines may appear desirable, it may not be necessary to restructure the Community in this fashion to achieve the intelligence integration vision described above. However, AFCEA recognizes that neither of the current models (individual agency initiatives; Community-sponsored architecture with individual agency implementation) is sufficient to make real the vision of the HISSG or the DCI.

AFCEA recommends a third model, one that has already proven itself effective in the private sector, takes advantage of emerging information technologies as they become available, and focuses complex value chains on satisfying a wide range of customers.[1] This model allows for the continued autonomy of major components of an industry. At the same time, the model creates *new business processes* serving a wide variety of participants. The rise of business-to-business (B-to-B) exchanges that link data, create knowledge, and allow for swift transactions among a wide variety of participants, is an example of this model. Some of these exchanges encompass entire industries. For example, Covisint serves a wide range of automobile manufacturers, parts manufacturers, and other automotive supply chain participants. Using common data standards, participants can post their need for parts, evaluate bids, integrate basic order management, and even gain visibility into selected components of each other's supply and value chains. Covisint was formed by DaimlerChrysler, Ford, General Motors and Renault-Nissan and today includes PSA Peugeot Citroen. Covisint was formed to reduce waste and improve customer response. The automobile industry found that asset use was less than 50 percent in some cases, even as customer expectations regarding product variety and quality continued to rise. A host company can use the Covisint community portal, or Covisint can customize a portal that can extend a customer's current enterprise systems out to its suppliers in a safe and secure manner. In essence, the Covisint B-to-B model allows for the flexible configuration of "extranets" serving a variety of participants. Since its inception in 2001, Covisint has serviced more that $150B worth of on-line transactions. More than 25,000 organizations (manufacturers, suppliers, industry groups) are registered with the exchange, encompassing more than 120,000 active users. This model, serving an entire industry, relies on standardized interfaces, coverage of an entire value chain, relevancy for players all along the value chain, and very low transaction costs.

Other, more modest examples of this model exist. The Houston Street Exchange offers a system for trading of wholesale electricity, crude oil, and refined products. RateXchange provides a multilateral bandwidth exchange for the telecommunications industry. In a variety of industries, B-to-B exchanges and secure technologies allow a variety of participants to share business processes along their entire production lines, to create new business processes, and to provide their customers with new products. Perhaps even more important, these exchanges enhance the concept of "mass customization" (by which large enterprises can customize products using a common, enterprise infrastructure) over several infrastructures. The Intelligence Community is

[1] See "The Future of Competition," by C. K. Prahalad and Venkat Ramaswamy. The authors describe how new information technologies create value for customers by integrating the processes of complex infrastructures. This integration enables process and organizational changes, but it does not require those changes be made in advance of the use of the technologies that enable this integration.

faced today with the need to support a growing customer base interested in a dynamic range of issues. Intelligence resources at all levels are expected to provide national and tactical product. Joint operations required a fused image of the operational environment segmented by intelligence discipline. The Global War on Terror requires the Community to provide as seamless as possible a view of the threat environment, capable of revealing complex and subtle relationships among a shifting pattern of regional and global players. The provision by each traditional intelligence infrastructure of "refined" product for top-level fusion does not suffice in this environment. In contrast, users need a more complete and organic view of the situations they face in real-time. Such a requirement compels the Community to search for new business processes that provide collaboratively created products at all levels. The recent capture of Sadam Hussein highlights the need for a complete intelligence picture created within the decision and execution loops of the operators. The Community needs processes to provide such intelligence reliably and consistently.

A number of commercial supply chain technologies have already been demonstrated as effective aids to the management of Intelligence Community resources. Oracle and i2 supply chain management and optimization tools have been applied by components of the cryptologic community. In both cases, the extent of software customization required to model and optimize cryptologic resources was no greater than is typically required to use these tools in private sector industries. A study of the SIGINT Reference Model, contrasting it to commercial value chains, found a number of segments of the cryptologic system that are analogous to segments of commercial value chains, and no less likely to benefit from the use of the commercial supply technology by their commercial segment counterparts. The use of these technologies, focused on optimizing resources in support of customers, is consistent with the vision described above: *"end-to-end management and integration of information and intelligence functions,"* in support of a *"consumer-centric construct."*

This third model, although not requiring the organizational integration of existing, discrete infrastructures, does require a high degree of cooperation, collaboration, joint development, agreement on common business processes at a wide variety of points along each participant's value chain, and recognition of the value resulting products bring to customers. In the case of Covisint, the various industry players (GM, Ford, DaimlerChrysler, Renault/Nissan, etc.) built a joint venture, provided it with resources, and empowered it with the right to survey and connect to existing information systems in companies that view each other as competitors. The program office was provided an objective, as well as resources and authority, to create the exchange required. Consistent with sound business process engineering, business processes to be combined or created were defined and made subject to agreement before implementation. Team members were provided with routine access to information systems (and information) and operated with a distinct identity, rather than as visiting representatives of a competing organization assigned temporarily to the program office.

Perhaps even more important, an integrated capability could give rise to new concepts of operation in which collection, exploitation, processing, analysis, reporting, and dissemination would take place in ways not today envisaged. The history of rapid technology adoption in the

private sector provides numerous examples of processes created as a result of the opportunities offered by new, enabling technologies. In many cases, these processes were unanticipated and change fundamentally and beneficially the products they support. In some cases, these processes can give rise to a new discipline more powerful than the individual disciplines from which it arises. The Intelligence Community may be able to create an *integrated intelligence discipline* that provides national security decision-makers and operators with a new set of integrated intelligence products that fulfill the vision of the Community's leaders.

The technology, organizational approach, and industrial capacity to accomplish integration of the Intelligence Community, without having to combine existing infrastructures, exist. Nonetheless, significant impediments to this integration exist. The Intelligence Community must overcome these impediments if it is to achieve the integration vision of the Community's leaders.

Overcoming Impediments to Integration

Security Processes

Security processes and structures within the Community and its industrial partners continue to impede the efforts to combine existing business processes, to create new business processes, and to bring to bear the industrial capacity required to support the integration. Individual programs within each separate intelligence infrastructure are segmented through a variety of special accesses. Processes of crossing security clearances and accesses from agency to agency, particularly for industry people, remain slow and inconsistent. The requirement that people must be cleared before they work on important programs continues to limit to a small subset of the industrial resources available to support the Community and its integration. Investments needed to clear personnel and create secure (SCIF) environments are expensive, sometimes deterring desirable industrial participation.

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") are offering separately a paper[2] that addresses these security concerns. That paper recognizes implicitly both the emerging vision of horizontal integration and the industrial/technological opportunities that exist to support that vision. The paper makes a number of focused recommendations to reduce significantly the clearance logjam that confronts both this vision and these opportunities.

Industry recognizes the need for Intelligence Community organizations to maintain robust security programs and infrastructure. Therefore, in addition to making recommendations, the Community should create a cadre of "Community" participants whose clearances would be maintained by an office not subordinate to an individual agency. These clearances and accesses would be recognized Community-wide. At a minimum, adjudication of clearances and granting

[2] Improving the Security Clearance Process Through Automation and Common Criteria: A White Paper on Issues Confronting the Government Contractor Community

of accesses to people involved should be managed at the Community level. A process is needed by which integration personnel can be granted special accesses on an expedited and consistent basis. The Community as a whole should constitute a working group with sufficient resources to reduce significantly the backlog of clearances that continues to hinder industry participation. Finally, the need for SCIF facilities should be examined. That examination should compare the risks associated with a more permissive physical environment for system development with opportunity cost in useful intelligence paid by the Community in insisting on system development using a separate physical infrastructure.

Program Organization

The IC-MAP effort highlights some of the difficulties associated with placing a program office within an existing agency member of the Community. Progress in the IC-MAP program, while laudable, has been impeded by a lack of authority by which the program management office can gain the participation of Community members.

A program office that reports directly to the Community's leadership should manage the creation of an integrated Community capability. Its resources should be budgeted discretely, not as individual line items within the budgets of the member agencies. The business processes it defines in concert with member agencies should be submitted to and approved by the Director, Central Intelligence.

System Architecture and Engineering

The development of integration capabilities requires adopting an architecture that is sufficiently open. The architecture should allow the flexible addition of new technologies while being sufficiently disciplined to ensure straightforward connectivity. The Community should look to industry for a definition of an overarching architecture for collaboration at all levels of the various value chains represented by today's discrete intelligence infrastructures. The Community's leadership should adopt that architecture and associated technical standards. System engineering of new systems (and significant changes to current systems) should have on its critical path the development of integration capabilities. Program budgets, plans, and milestones should reflect the dependency that new systems under development have on integration capabilities. Individual system concept of operations and business process development that take place prior to system engineering, and design should be derivative of concepts of operations and businesses processes approved by the Community's leadership in support of horizontal integration.

Statute and Regulation

AFCEA recognizes that the various intelligence disciplines today are governed both by overarching law and regulation as well as legal and regulatory structures specific to each discipline. The establishment of new, integrating business processes should be followed swiftly

by an examination of applicable law and regulation by a senior legal counselor to the DCI to assess what changes might be made to implement these new business processes.

This paper provides a supplemental series of recommendations regarding legal and statutory issues that should be addressed to facilitate integration.[i] We offer this supplement to facilitate early legal analysis by the senior counselor, the appointment of whom we recommend above.

Summary of Recommendations and Proposed Timeline

Using the third model as described, the Intelligence Community should move swiftly to achieve the integration vision described by the HISSG and DCI. Doing so would advance the implementation of integration as defined by the HISSG and DCI, while enabling additional steps toward the development of a new, integrated intelligence discipline. Both our national security imperatives and the technological opportunities available for integration argue for swift implementation.

- The USDI and Chief, Community Management Staff (CMS), should immediately request an adjustment to the FY05-09 IPOM/IBES to accommodate the integration defined in this paper. The Community should immediately adjust input to the IPOM/IBES to reflect the establishment of an integration program office. The Community should request from Congress a supplemental appropriation for FY04 for the establishment of that office. If it is too late to change the FY05-09 IPOM/IBES, the Community should make changes to the FY06-10 IPOM/IBES and modify the FY05 budget request to continue the efforts to be started in FY04.
- Within 60 days, the Community should establish an integration program office. To the extent possible, the office and its organizational structure should reflect the approaches used by the private sector in building business to business exchanges, approaches in which disparate, and sometimes competitive organizations, build a common system for a common goal. The program office should undertake further development of the specific actions necessary to implement these recommendations, which are high-level in nature. If a government acquisition context is employed, the program office should consider the use of the DoD advanced concept technology demonstration (ACTD) or advanced technology demonstration (ATD) approaches to enable swift, incremental adoption of these recommendations.
- The program office should have its own acquisition organization and executive.
- The DCI and USDI should consider requesting from a Congress a funding approach that avoids embedding this effort within the Intelligence Community's existing funding mechanisms. The recommended third model approach would make the integration program office responsible to both DCI and the Secretary of Defense, with its own Office of Management and Budget budget line.
- With support from the Intelligence Science Board and others as appropriate, the program office should survey available commercial technologies and business models that could be applied within the next 24 months to facilitate the integration of intelligence.

- The program office should be authorized when established to promulgate top-level data and protocol standards for use in integrated business processes. The program office should consider work already done by members of the Community to define these standards.
- The program office should work with the senior counselor to the DCI described above to define legal and regulatory approaches to horizontal integration. This task should be accomplished within 12 months.
- The program office should provide to Congress an FY05 budget submission for horizontal integration capabilities and IPOM/IBES input for FYDP funding of those activities.
- The program office should present to the DCI and USDI within 12 months a program plan (plan of actions and milestones) with increments of integration capability, modifications to the architectures of existing programs and programs underway in Community member agencies, timelines, and budgets.

Conclusion

The integration of intelligence, leading to new, collaborative business processes capable of supporting national security decision-makers and operators, is now technically possible. Models for business process and value integration already exist. Significant, but not insurmountable, impediments exist that must be addressed and resolved to achieve this integration. Intelligence Community leaders have already defined an integration vision. To achieve that vision, AFCEA urges immediate action to create the Integration Program, change ongoing IPOM/IBES and budget submissions, and press forward with the legal analysis started in this paper's supplement. The nation needs no less.

Supplemental - Legal and Statutory Issues Relating to Horizontal Integration

[i]

When Congress passed the National Security Act of 1947 it made clear its intention regarding the integration of the Intelligence Community:

"In enacting this legislation, it is the intent of Congress to provide a comprehensive program for the future security of the United States; to provide for the establishment of integrated policies and procedures for the departments, agencies, and functions of the Government relating to the national security…" (Ref: 50USC Chapter 15, Sec. 401) (Emphasis added.)

However, over the past three decades as a federation of agencies and organizations with mostly legally autonomous missions and with the authorities to self-direct individual security management programs, the Intelligence Community has evolved as other than an integrated enterprise.

Today there are a vast number of laws and regulations that specifically impede or prevent the ability of the federal government to foster an integrated Intelligence Community, one that relies on standards, tools, engineering and architecture, particularly the integration of intelligence itself as a discipline with specific rules of engagement for intelligence data and information sharing. There are many opportunities for conflicts in the execution of authorities regarding data protection and data access that can frustrate and/or prevent horizontal integration in general or on a mission-specific basis.

Although the technical and operational recommendations in the main body of this paper can be undertaken in stages, with some elements addressed in the short term, we recommend three broad steps – within the legal and statutory context - to enable integration:

- First and foremost a rigorous review of the intent and implications of existing laws and implementing regulations that govern the Community, with particular attention to the changing authorities embedded in the National Security Council as each Administration defines its perspective of the role of intelligence in national security through the issuance of National Security Presidential Directives
- Second, the identification and codification of an operations model to create the intelligence enterprise
- Third, adoption of the design and use of performance metrics to adjust the legal framework, as needed, based on performance results.

The key laws governing the Intelligence Community that provide authority, accountability and responsibility mandates for safeguarding the security of the United States are: Title 10, United States Code (Armed Forces); Title 50, United States Code (National Security Act of 1947); and more recently, The Patriot Act. These laws are balanced in part by the Constitutional rights of U.S. persons to free speech (First Amendment) and to protection against search and seizure (Fourth Amendment) and by the Privacy Act of 1974.

There are two specific issues for review in the legal framework: conflicts in the authorities, accountabilities and responsibilities provided to management positions; and barriers to mission accomplishment caused by individual security programs.

First, a thorough analysis should be conducted of the present authorities set forth for key management positions within the Intelligence Community. To begin this effort, the following positions and defined roles regarding the control of intelligence data and information should be scrutinized with an eye toward modifications needed to create an integrated enterprise:

Director, Central Intelligence

- DCID 1/7, "Security Controls on the Dissemination of Intelligence Information," June 30, 1998

- DCID 6/4, "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI)," July 2, 1998)

Intelligence Community Chief Information Officer
- DCID 1/6, "Intelligence Community Chief Information Officer," February 4, 2000)

Secretary of Defense
- DODD5105.42, "Defense Security Service (DSS)," May 13, 1999)

Deputy Under Secretary of Defense (Policy) (DUSD(P))
- DODD5240.1, "Activities of DOD Intelligence Components that Affect U.S. Persons," April 25, 1988)
- DODDD5200.39, "Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection," September 10, 1997)

Assistant Secretary of Defense (C3I) [now Networks & Information Integration (NII)], as the DOD Chief Information Officer
- DODD8000.1, "Management of DOD Information Resources and Information Technology," February 27, 2002)
- DODD8320.1, "Data Elements and Data Codes Standardization Program," September 26, 1991)
- DOD8500.1, "Information Assurance," October 24, 2002)
- DDOD8520.1, "Protection of Sensitive Compartmented Information (SCI)," December 20, 2001)

The OSD Principal Staff Assistants and the Chairman of the Joint Chiefs of Staff
- DODD5015.2, "DOD Records Management Program," March 6, 2000)

The Chairman, Joint Chiefs of Staff shall
- DOD5030.59, "National Imagery and Mapping Agency (NIMA) Limited Distribution Imagery or Geospatial Information and Data," May 23, 2003)

The Heads of DOD Components
- DODD5205.8, "Access to Classified Cryptographic Information," February 20, 1991)

Director, National Security Agency/Chief, Central Security Service
- DODD5100.20, "Administrative Reissuance Incorporating Through Change 4," June 24, 1991)

Director, National Imagery and Mapping Agency (NIMA)
- National Security Act of 1947
- EO 12333; EO 12951 and EO 12958
- Presidential Decision Directive NSTC-8

Director, Defense Intelligence Agency
- DODD8520.1, "Protection of Sensitive Compartmented Information (SCI)," December 20, 2001)

Secondly, the impact of the following Executive Orders on the sharing of intelligence information and data needs to be examined, with one focus being the removal of barriers between and among the individual security programs:
- EO 12333, "United States Intelligence Activities," 04 December 1981
- EO 12829, "National Industrial Security Program, " 06 January 1993
- EO 12958, "Classified National Security Information," 12 April 1995
- EO 12968, "Access to Classified Information," 02 August 1995
- EO 13292, "Classified National Security Information," 25 March 2003

- EO 13311, "Homeland Security Information Sharing," 29 July 2003

There are many opportunities for conflicts in the execution of authorities regarding data protection and data access that can frustrate and/or prevent horizontal integration in general or on a mission-specific basis. Each entity of the Intelligence Community is authorized to have its own security program (Executive Order 10450). In addition, by law, a National Industrial Security Program (EO 12829) for safeguarding classified information (EO 12356) is applicable to all executive branch departments and agencies.

The culture of the security management system that has devolved from these authorities is strongly risk averse and operates with little if any intervention by the management levels within the Department of Defense.

As a consequence, the Chiefs of Security of each of the IC components and of DOD industrial security have considerable discretion in use of authority, as delegated, to select the classification levels for intelligence data and the rules governing access to such data. This distributed security management system that favors risk aversion can disrupt achievement of enterprise and horizontal integration and, in particular, frustrate effectiveness and efficiency in time-sensitive tactical operations. Notwithstanding use of Director, CIA's Directive 6/6 for ORCON and of the Director, NSA's Directive 18 for SIGINT protection, there may be instances where such authority should be considered through rules of engagement for intelligence data and information sharing that are based on risk management.

An approach that may be worth considering is to scrutinize the use of data that provides information that is openly obtained and information that is obtained under classified operations. For the former, referred to simply as "information," reliance on rules carrying incentives for risk management could lead to greater data accessibility and possibly lower levels of classification. For the latter, where sources and methods would be obtained/performed using classified means, the sources and methods could retain the title of "intelligence," with high classification levels and access restrictions and the findings determined to be "information," with greater flexibility in access and classification rules applied.

To summarize, transformational change of the nature required to achieve the integrated policies and procedures envisioned by the National Security Act of 1947 and that facilitate the efficient and effective execution of any of the business models offered herein must be decreed from the top. Based on an understanding of the restraints resulting from the current legal framework, the White House, Secretary of Defense, Director Central Intelligence and the Congress should set about to create a new legal framework that will permit the development of an integrated intelligence enterprise.