



Market Brief

*The Private Sector's Role in Building the Intelligence
Community of the 21st Century: Increased Partnering with
Industry to Maintain America's Edge*



Equity International/Chesapeake Innovation Center

March 2005





Summary

The U.S. Intelligence Community (IC) is dramatically increasing its outreach to industry, offering an emerging and fast-growing opportunity for businesses of almost all sizes and categories. Driven by factors such as the convergence of homeland security, military, and intelligence requirements and the challenge of analyzing a tidal wave of digital information, the IC has expanded the size, number, and variety of its contracts with the private sector. This trend is likely to increase as IC spending ramps up and the recently passed Intelligence Reform and Terrorism Prevention Act of 2004 speeds standardization and technological research at a community-wide level.

The IC budget, estimated at \$40 billion [1], is approximately that of the entire budget of the Department of Homeland Security (DHS) and appears to be growing at least as quickly as that of DHS and the FBI (the Bush Administration's FY 2006 request for DHS is \$41.1 billion) [2]. In comparison with last year's budgets, the Bush Administration has requested a 7 percent increase for DHS (excluding Project BioShield) and 11 percent for the FBI.

Addressable Spending May Approach \$10 Billion Annually

It is important to bear in mind that the budget of a government activity is not the same as the market created by it. "Addressable" spending— expenditures not accounted for by overhead, normal payroll, internal operations, and other activities conducted without private sector assistance – is one measure of the market for potential contractors. One 2005 media report estimated that up to \$20 billion of the IC's annual spending is addressable; the authors believe that estimate is far too high. In its authoritative study on homeland security spending, the Civitas Group pegged addressable intelligence-related spending at \$27.6 million over a five-year period starting in 2004 [3]. However, based on comparisons with other federal agencies and analysis of publicly available contracting information, the authors believe the IC's addressable spending may approach \$10 billion a year (because of sensitivities involving intelligence budgeting, this report generally does not attempt to break down spending categories more specifically). Whatever the precise numbers, there is no doubt the IC is creating many billions of dollars in new procurement opportunities.

For example, from 2000 to 2004, the National Security Agency –said to be the largest of the 15 agencies making up the IC – doubled its procurement spending and will do so again by 2010, according to a senior agency official [4]. An Agency representative has stated the NSA executed 36,000 procurement actions in FY 2004, creating billions of dollars in procurement obligations. In effect, the NSA alone is a multi-billion market.



Members of the IC

The IC is generally considered to consist of 15 member agencies. In the public's imagination, the IC is often associated with civilian agencies such as the CIA. In reality, most of the IC is linked to the military. The 15 IC agencies are: Army, Navy, Air Force, and Marine Corps intelligence organizations that provide intelligence required by each service; Central Intelligence Agency (CIA) which supplies national leaders with foreign intelligence; Coast Guard Intelligence which focuses on intelligence involving maritime security; Defense Intelligence Agency (DIA) which provides intelligence to military commanders; Department of Energy which analyzes nuclear and energy-related intelligence; Department of Homeland Security (DHS) which handles intelligence to help prevent terrorist attacks within the United States; Department of State which focuses on intelligence affecting U.S. foreign policy; Department of Treasury that follows terrorist financing and issues involving US monetary policies; Federal Bureau of Investigation (FBI) which focuses on counter-terrorism and counter-espionage; National Geospatial-Intelligence Agency (NGA) which provides geographic intelligence such as images and maps; National Reconnaissance Office (NRO) which is in charge of coordinating airplane and satellite reconnaissance; and the National Security Agency (NSA) which collects signal intelligence and protects IT systems.


The CIA, DIA, NSA, NRO, and NGA are wholly devoted to intelligence. The remaining organizations have other missions, but also units responsible for intelligence and part of the IC.

Drivers of the Intelligence Market

More than ever, "connecting the dots" is considered key to preventing terrorism, defeating America's enemies in the GWOT (Global War on Terrorism), and achieving other vital national security objectives. From the battlefields of Afghanistan to the secure facilities around the Washington D.C. Beltway, IC officials are struggling with an unprecedented "volume, velocity and variety" of data, causing what is referred to as the problem of "information overload." A senior intelligence official has called this a "tidal wave" of data, saying: "We can either be drowned by it or we can get on our surfboard and surf it and let it propel us. And, of course, that's what we're trying to do."

Following cutbacks in the 1990s, the IC was already transforming before 9/11. But its members were galvanized by the terrorist threat and IC shortcomings were revealed when the Community failed to predict the 2001 attacks or provide accurate reporting on WMD in Iraq. The IC is now undergoing substantial growth and change driven by a number of factors, including:

- Increasing federal spending: While classified, the IC's budget appears to be growing substantially and is at least on par with the Department of Homeland Security and FBI (as a whole, including its intelligence and other operations).
- Requirement to keep pace with commercial technology: America's enemies now have



the assets of the world's commercial technology market at their fingertips, providing them with new, sophisticated ways to communicate, launch cyber and physical attacks, collect intelligence on the United States, and avoid detection. This requires the IC to employ the commercial sector to stay ahead.

- Shifting contracting and R&D practices: Responding to requirements to enlist the private sector in transformation, the IC has launched a variety of initiatives to increase the scope and breadth of contractor support, including the acquisition of innovative high technology, the attraction of disadvantaged businesses, and the positioning of IC agencies as good customers. Much of the billions being spent by the IC in outsourcing involves huge and often classified projects by major defense contractors. This is part of a larger trend, exemplified by the \$2 billion, 10-year "Project Groundbreaker" contract started in 2001 to upgrade the NSA's IT infrastructure. However, smaller subcontractors used by these large corporations represent a significant part of the market. In addition, members of the IC are significantly increasing their own contractor pools, adding thousands of small- and medium-size vendors.


In the mid-1990s, according to an NSA official, about 20 companies did 85 percent of the Agency's contracting. However, over the last several years, the NSA alone has increased the number of its contractors from 140 to more than 2,690; In FY 2003 the Agency conducted 43,000 contracts and 21,000 purchase orders [5]. Industry outreach activities by other IC members suggest a similar trend in their procurement activities. The appointment of NSA director Air Force Lt. Gen. Michael Hayden — a leading advocate of IC transformation and increased industry involvement — as Deputy Director of National Intelligence indicates the likely expansion of this trend.

- Convergence with the homeland security mission: The lessons of 9/11, combined with the easing of the regulatory barrier known as "The Wall" between the IC and domestic law enforcement, has given the IC an increased role in supporting domestic security. This includes providing intelligence support and expertise to other federal, state, and local agencies, and selected private sector organizations. IC veterans are helping to transform law enforcement at federal and local levels; the FBI's new Executive Assistant Director (EAD) for Intelligence and Chief Technology Officer are both senior veterans of the National Security Agency, while intelligence veterans are training numerous local agencies.

DHS is growing its own intelligence capabilities and by one report plans to spend \$431,900,000 for intelligence and warning under its FY 2006 requested budget, a 23.5 percent increase over FY 2005 (this does not include classified spending by the intelligence community) [6].

In addition, the NSA has assumed a leading role in improving cyber-security.

- Convergence with military operations: The rapid collection and dissemination of intelligence is a key feature of overall military transformation and "data-centric" strategies. This is driving IC work supporting special operations, itself a booming market linked closely to




elements of the IC, and huge transformational projects such as the GIG (Global Information Grid).

- Intelligence Reform and Terrorism Prevention Act of 2004: The Intelligence Reform Act does not create massive new spending in the IC. Indeed, much of its \$2 billion in new authorized funding is for agencies such as the Border Patrol and Transportation Security Administration. However, the Act seems likely to speed the opening of the marketplace by increasing the prioritization and standardization of the IC and vesting power in the new Director of National Intelligence. “These authorities vested in a single official who reports directly to me will make all our intelligence efforts better coordinated, more efficient, and more effective,” said President George W. Bush. This Act also includes the creation of an Information Sharing Environment (ISE) to allow the distribution of terrorism information to governments at federal, state and local levels, along with selected private sector entities; up to 500 new personnel for the DNI’s office, including a senior technology official; and measures to protect civil liberties (dealing with a serious constraint in the market as discussed below).
- Dual-Benefit Technology Development and Commercialization: The unique data mining software that helps an IC agency detect terrorist activity today may be modified to help a major corporation control its inventory tomorrow. Conversely, technologies now transforming the corporate sector may be adapted to the IC’s missions. IC spending is also spurring the development of an “Informatics Corridor,” centered in Anne Arundel County, Maryland, (home to the NSA) and stretching to the National Institutes of Health (backers of bio-informatics research) in Maryland, DHS and FBI in Washington D.C., CIA in Northern Virginia, and other IC members around the Washington Beltway. Growth by the IC and prime contractors is creating a real-estate boom in certain areas of Anne Arundel County. IC demands for new technology, supported by research at local institutions such as the University of Maryland and Johns Hopkins University, are generating new business activity by entrepreneurs and mid-tier companies, drawing interest from around the world and creating an industry hub focused on informatics, knowledge discovery, and information assurance software.

Areas of Spending

Certain major areas will provide the greatest opportunities for private sector involvement. They include:

- Technology integration and program support: While information on much of this spending is classified or otherwise not publicly available, IC agencies are spending hundreds of millions of dollars a year for technology integration services.
- Human capital: The IC is adding at least 2,000 employees a year. The NSA announced in 2004 it would hire 1,500 new personnel a year for five years. The NGA reportedly seeks to hire 900 new analysts. In November 2004, President Bush ordered the CIA to increase the number of analysts, case officers, and linguists by 50 percent. According to media reports,



the FBI may be hiring 4,000 new employees; the Bureau itself has launched an advertising campaign to recruit hundreds of intelligence analysts. This creates numerous opportunities for the private sector, including training, human performance and organization improvement, HR, and recruiting services.

- Personnel outsourcing: There are simply not enough qualified and “cleared” (those with active security clearances) personnel to serve the needs of the IC. Organizations specializing in the provision of contract employees for the IC (sometimes known as “body shops”) report a surge of new business. One boutique firm has grown from 84 to more than 200 employees over the last year by providing operational and analytical specialists to the IC. Staffing giant Kelly has set up a unit, Kelly FedSecure, solely devoted to providing cleared personnel
- Data: For example, the NGA has awarded contracts worth up to \$750 million for three companies to provide it with high-resolution satellite images. The IC is also purchasing public record data from the huge and rapidly expanding private information industry.
- Equipment: From satellite equipment to supercomputers, the IC investment is in the billions of dollars. While much of this equipment is highly specialized and provided by a small number of major contractors, the IC must equip its thousands of new employees and new facilities, creating significant opportunities for vendors providing everything from office software to modular furniture.
- Innovative technology: IC agencies are seeking innovative solutions in areas such as informatics technology, knowledge discovery, data mining, visualization, collaboration, information assurance, remote sensing, advanced computing and knowledge management.

M&A and Early-Stage Financing Propelled by the IC

The growth of the IC market is also contributing to M&A and investment activity. So far this year alone, there have been at least \$750 million in acquisitions of companies linked to the IC (Lockheed Martin acquiring The Sytex Group; Northrop Grumman buying Integric Corporation; Essex Corporation purchasing The Windermere Group). ChoicePoint — a multi-billion dollar company that aggregates vast stores of data and operates complex information sharing networks — has been snapping up dozens of companies, including those with intelligence customer connections. Its competitor, LexisNexis Group, reportedly a provider of public records to the CIA, last year purchased Seisint Inc. for \$775 million (which supports the Matrix information sharing system) [7].

The growth of this sector is also driving increased venture capital, early stage investing, and high-tech venture creation. For example, In-Q-Tel, the CIA-supported venture capital group, says it has invested more than \$150 million in promising emerging technology companies. Paladin Capital Group, whose principals include a former director of the NSA, closed its second

homeland security fund for \$235 million last year. The Maryland Technology Development Corporation has focused on supporting a number of start-ups serving the IC.

Market Constraints/Barriers to Entry

While a market of great potential, the IC continues to present challenges to private sector enterprises trying to serve it.

- Dependence on federal spending: At some point, the current increase in federal support of the IC will slow. However, the authors believe current spending patterns will continue for at least three years.
- Fragmentation: Contracting remains dispersed among the various IC members and prime contractors and over-arching priorities are limited (this will likely be improved by the addition of the DNI to the planning process).
- Procurement process and bureaucracy: Both the IC agencies and their contractors conduct procurement through sometimes complex, risk-averse, and slow-moving bureaucracies that often present an advantage to contracting incumbents. This system can be especially onerous for small companies that may not have the resources to undertake procurement processes lasting many months.
- Classification requirements: Although substantial unclassified contracting opportunities exist with the IC, the process for a company to acquire an organizational security clearance and retain cleared personnel is often lengthy and expensive. While the Intelligence Reform Act and agency initiatives will improve the situation, industry experts believe improvements will be slower than anticipated and that bureaucratic resistance, employee churn, and a graying federal workforce – which will lose thousands of cleared personnel to retirement in coming years – will ensure a scarcity of cleared employees well into the future.
- Existing IC Capabilities and Requirements: In some cases, IC capabilities may exceed those of private sector enterprises seeking to assist. For example, according to an NSA official, after 9/11 a leading Silicon Valley company that offered assistance found the Agency's challenges far beyond its capabilities. In other areas the NSA and other IC members most likely already possess the most advanced solutions in the world.
- Privacy, civil liberties and public policy concerns: The disconnect between the IC and law enforcement communities that prevented the United States from connecting the dots before 9/11 stemmed in large part from limitations enacted after abuses in the 1970s. Modern American society has a growing interest in privacy and control of personal data. These factors negatively impacted the Total Information Awareness (TIA) and Computer-Assisted Passenger Prescreening System (CAPPS-II) programs. Concerns about IC outsourcing have also been raised in connection with the prisoner abuse scandals in Iraq and Afghanistan. While the Intelligence Reform Act and other initiatives focus on addressing these issues, new scandals could disrupt the growth of the market.

- Standards: The intelligence community is highly sensitive to standards not simply for policy or legislative reasons, but most importantly for security reasons. Much of the private technology development will be subject to proprietary standards that ensure operational security and interoperability. Meeting such requirements can be expensive and time consuming, especially for small companies.

Purpose

This market brief is designed to help the leaders of commercial organizations determine how they may assist U.S. government agencies achieve their missions and build the intelligence organizations required to protect America from the threats of the 21st Century.

About Equity International and the Chesapeake Innovation Center

<http://www.equityinternational.tv> ; www.cic-tech.org

Equity International (EI), a prominent Washington business development firm, is the leading U.S. facilitator of business involvement and solutions in homeland security. It is the organizer of the 2005 Homeland and Global Security Summit. The Chesapeake Innovation Center (CIC) is America's first business accelerator for homeland and national security.

The Authors

Jeffrey Wells is an independent international business and market analyst. His background includes experience with international corporations, state and local government organizations, military and intelligence organizations, trade missions, and economic development organizations, as well as angel and venture capital sources. Mark Sauter, COO of the CIC, has worked as a senior executive in several venture-capital backed start-ups and was formerly an award-winning journalist. He also served as an Army officer with infantry and Special Forces units.

Disclaimer and Sources: This brief is copyrighted by EI and the CIC. Reproduction of this report in whole or part is prohibited without the written permission of the copyright holders. The research in this report reflects the authors' opinions as of the date of publication and carries no guarantee of accuracy. The contents are not intended as a guide to investment and the copyright holders, authors, EI and the CIC, their employees, officers and directors, are not liable for any loss related to this report.

Certain companies or government organizations mentioned in this report may have business relationships with EI and/or the CIC. This report is not intended to reflect the views of any organization affiliated with EI and/or the CIC. The information in this report has been obtained from unclassified, open sources.

Information from this report was published in The Washington Post, March 6, 2005, "Cracking the Code to Security Contracts"

<http://www.washingtonpost.com/wp-dyn/articles/A12184-2005Mar6.html>

Contact: Melanie Dougherty, 202-486-1182



References

1. \$40 billion IC budget estimate is based on numerous sources, including the Congressional Research Service. While the current IC budget is classified, the U.S. government did release the FY98 total of \$26.7 billion; growth in the ensuing years supports the current approximation of \$40 billion.
2. Not just one of the federal government's largest spending areas, the IC budget dwarfs such major industries as the U.S. publishing business (sales of \$23.7 billion in 2004), U.S. music industry (sales of some \$11 billion in 2003), and U.S. machine tools (2004 "consumption" estimated at approximately \$3 billion). Data from industry associations.
3. "The Homeland Security Market," Civitas Group LLC, June 2004.
4. "Security agency doubled procurement spending in four years," Govexec.com, June 1, 2004.
5. Id.
6. "The FY 2006 Homeland Security Budget Request: Key Implications for the Private Sector;" Civitas Group LLC, Feb. 2005.
7. "In Age of Security, Firm Mines Wealth Of Personal Data," Washington Post, Jan. 20, 2005.