Ideas for America's Future
Core Elements of a
New National Security Strategy

By
Jeffrey P. Bialos

Co-Contributors
Stuart L. Koehl, David M. Catarius and Suzanne E. Spaulding
Chapter 15

Intelligence Reform: Matching Commitment to Imperative

The ink had not dried on the National Security Act of 1947 before the calls for intelligence reform began.\textsuperscript{366} Over the years these calls have prompted new legislation, including the Central Intelligence Agency Act of 1949,\textsuperscript{367} the reforms prompted by the Church and Pike Commissions, a series of changes embodied in Intelligence Authorization Acts,\textsuperscript{368} and, most recently, the Intelligence Reform and Terrorist Prevention Act of 2004 (IRTPA).\textsuperscript{369} Legislation emerging from these recommendations has often focused on organizational changes, however, in large part because reorganization is easier to mandate through legislation than is true reform.

Thus, in 1996, legislation created four new senior positions in the intelligence community designed to strengthen the community management role of the Director of Central Intelligence (DCI). These positions were resisted by the DCI, however, and nearly 8 years later only two of the four positions had been filled.\textsuperscript{370} The legislation also enhanced some of the authorities of the DCI under the National Security Act of 1947. Most observers agree, however, that these enhanced authorities, too, were never fully exercised. While some improvement was made, particularly through efforts like those of the Assistant Director of Central Intelligence for Collection aimed at innovative approaches to hard targets, subsequent reports found that the DCI was still not adequately bringing all elements of the intelligence community to bear on providing accurate, actionable\textsuperscript{371} intelligence to U.S. government decision makers.

In short, observers who seek to reorganize the overall U.S. national security apparatus (as discussed in Chapter 12) in order to advance national security policy “outputs” should recognize that organizational fixes alone may not be the answer, and will not necessarily improve intelligence. Despite multiple organizational changes over several decades,

\textsuperscript{366} While the 1947 Act restructured the overall national security apparatus and created the NSC (as discussed in Chapter 15), it also reorganized the intelligence community and created the CIA. For a summary of the many reform proposals over the years, see Best, Richard A. Jr., Proposals for Intelligence Reorganization, 1949-2004, Updated September 24, 2004, Congressional Research Service. Available at: http://www.fas.org/irp/crs/RL32500. pdf ("Best CRS Report").

\textsuperscript{367} 50 U.S.C.\$ 403.

\textsuperscript{368} See, for example, the Intelligence Authorization Act of 1997, P.L. 104-293, October 11, 1996, that created the Deputy Director of Central Intelligence/Community Management and Associate Directors of Central Intelligence for Collection, Administration.

\textsuperscript{369} IRTPA, 50 U.S.C. 403 et. seq, created the position of Director of National Intelligence to serve as head of the intelligence committee as well as the National Counterterrorism Center and other centers.

\textsuperscript{370} Intelligence Authorization Act for FY 97. See Best CRS Report, p. 41.

\textsuperscript{371} “Actionable” intelligence is often interpreted to mean intelligence that can be used in immediate operational or tactical planning. As used herein, the action also includes the development of longer term strategy and strategic plans. In this sense, “actionable” means information specific and relevant enough to inform decision-makers of all kinds, including those focused on strategic issues.
the U.S. intelligence community still faces serious issues over how to improve perceived shortcomings in its output.

![The Imperative: Enhance the Quality of Intelligence](image)

True reform should be aimed not at merely improving the organization of the intelligence community (IC), which is not an end in itself. Rather, we should focus on improving the quality of intelligence. This kind of reform cannot be legislated. It requires effective leadership, a clear vision, and sustained commitment.

High quality intelligence is essential for the success of virtually every element of national security policy. We depend upon the intelligence community to:

- collect information using sensitive sources and methods;
- combine that classified information with relevant “open source” information and expertise; and
- provide thorough, rigorous analysis, information and assessments to decision-makers in national security arenas at the federal, state, and local levels that are as accurate, timely, and actionable as possible.

Nevertheless, Americans and, particularly, policymakers need to understand that it is unrealistic to expect the intelligence community to meet this standard with respect to every security and foreign affairs target all over the world at all times. Rather, the challenge is to maximize the effectiveness of intelligence capabilities so as to enable significantly better strategic and tactical awareness, understanding, and warning about today’s—and tomorrow’s—threats.

The 9/11 Commission Report delivered a significant blow to the public’s confidence in the intelligence community, and the depiction of intelligence as having supported the WMD case for war in Iraq dramatically undermined its credibility. Neither impression is entirely accurate. Intelligence community analysts identified the serious threat to the homeland posed by al-Qaeda and Osama Bin Laden many years before 9/11, and policymaker misuse of intelligence created an image of certainty about Iraqi weapons programs that was lacking in the many of the intelligence reports.

Nevertheless, the community is left needing to restore its credibility and the trust of the American people. In part that will come from improving the quality of intelligence. But it will also take increased transparency, enhanced oversight, and pro-active steps to reassure that analysis reflects intelligence rather than policy preferences at either end of Pennsylvania Avenue—or within the community itself.

Improving the Quality of Intelligence—Moving from Plans to Action

Enhancing the quality of intelligence requires strategic action in three core areas of the intelligence “enterprise,” which is, after all, a unique type of business:

- **Effective leadership and management in support of national priorities**—First, it starts at the top, with excellent leadership that clearly shares the commitment of the workforce to the mission and to ensuring that IC personnel are deployed and managed in a way that maximizes their potential. The IC requires strong management and reasoned decision-making by its leaders. This in turn requires limitations on administrative burdens—non-mission-critical demands from a growing central bureaucracy.

- **Workforce quality**—A second critical element in the success of any enterprise is the quality of its workforce. This has obvious implications for recruitment, hiring, training, deployment, and retention.

- **Freer flow of people, information and resources**—The third essential element for producing better intelligence in today’s dynamic environment is to enable a freer flow of people, information, and resources to enable the level of agility required to meet evolving threats that do not fit into static organizational structures or stovepipes. Networked threats require a networked response—not just technologically but in terms of fully and effectively tapping resources inside and outside the IC in order to understand and defeat these threats.

A high-quality and agile, interactive IC workforce enabled and empowered by effective and committed leadership will produce better intelligence.

Soon after Admiral McConnell came in as the Director of National Intelligence (DNI), he promulgated a 100-Day Plan for Integration and Collaboration in the Intelligence Community. A report on the results of that plan was released in July, 2007 and was followed with the release of a 500 Day Plan in October of 2007, taking the IC to the end of the current Administration. The DNI’s plans address, to varying degrees, all three of these essential objectives: effective leadership and management; a high quality workforce, and freer flow of people, resources, and information. They are weak, however, on setting out strategies for implementation and defining clear metrics for evaluating progress.

---

373 See http://www.dni.gov/100-day-plan/100-day-plan.pdf.

374 Office of the Director of National Intelligence, United States Intelligence Community (IC) 100 Day Plan for Integration and Collaboration, July 2007.
Excellent Leadership and Management in Support of National Priorities

The DNI was established to bring a greater unity of effort to the intelligence mission. This does not mean pulling in or replicating all elements of the IC within the Office of the DNI (ODNI). Nor does it mean eliminating the distinct cultures of these various entities. Rather, it means getting the 16 different elements of the community to work effectively together, maximizing the unique strengths and capabilities of each, to accomplish the mission. The most important aspect of effectively managing the IC is to ensure that national priorities take precedence over agency priorities.

Recommendations for Better IC Management

Enabling more effective IC focus on national priorities requires taking steps in a number of discrete areas discussed below.

Applying Goldwater-Nichols Logic to the IC

The Goldwater-Nichols paradigm previously discussed has direct implications for the IC. The primary benefit of Goldwater-Nichols reforms in the military was bringing greater unity of effort to accomplish the mission. As discussed above in Chapter 13, this was done in large part by reducing the role of the service chiefs to that of “recruiting, training, and equipping” the men and women in uniform. The operational activity of these individuals was then managed by the combatant commander to whom they were assigned. A key principle was to ensure that the military resources were maximized toward the same priority—established by the combatant commander in response to overall direction provided through the national chain of command—rather than each service deciding their own priorities.

Before the Goldwater Nichols reforms, the various military branches were not confident that the others would adequately meet their needs. Thus, for example, each wanted to develop its own air, sea, and ground capabilities. Similarly, in the IC, each element increasingly seeks the authorities and capabilities of the other if they cannot rely on other agencies to match their priorities and meet the needs of their mission.

For example, it has been reported that, while military and CIA units worked extremely well together at times in Afghanistan, there were times when the CIA unit at a given site would suddenly announce that it was leaving because this particular mission was no longer its priority and it was being re-directed elsewhere. The military unit, for whom that mission remained a priority, was left without adequate intelligence support.

Thus, we have seen DoD re-creating the entire intelligence community, including the full range of human intelligence (HUMINT) capabilities, in order to ensure that it has the intelligence necessary to meet its mission. DoD certainly has legitimately unique HUMINT requirements in the tactical arena. However, the lines between tactical and strategic are increasingly blurred, particularly in the counterterrorism context, expanding the scope of DoD’s intelligence efforts. With the Homeland Defense mission, the mili-
tary has even sought and received some domestic intelligence authorities, such as the use of National Security Letters, which were previously the province of the FBI.\textsuperscript{375}

The Goldwater-Nichols paradigm applies to the IC, where the heads or directors of the various IC elements (the CIA, Defense Intelligence Agency, etc.) are the equivalent of the pre-reform armed service chiefs. Just as Goldwater-Nichols shifted from the service chiefs to the combatant commander the authority to determine which troops did what and where, the DNI must take over from agency heads the authority and responsibility to ensure that national, rather than agency, priorities govern the activities of the intelligence professionals.

\textbf{Enhancing the DNI’s Budget Oversight and Management}

The most effective way to ensure national priorities are being met is for the DNI to have timely transparency into budget execution by IC agencies aligned by mission. The closer the DNI can come to having real-time budget execution data arranged by mission area, the more comprehensive will be his or her knowledge of how intelligence assets are deployed, how well all of the program and activities are fulfilling their missions, and whether they are meeting national priorities. This will also allow far more agile, efficient, and effective management of those resources, including reallocation of funds during the year of execution rather than primarily at the annual budget build. Technology should enable automatic transparency in budget execution across all agencies in the IC without burdening those obligating the funds with additional reporting requirements.

\textbf{Inverting the Pyramid: Limiting DNI’s Growth and Curbing Administrative Burdens that Hamper Efforts to Improve Intelligence}

The IRTPA was intentionally vague on many of the provisions describing the authority of the DNI. This reflects the political compromises necessary to win enough votes from a skeptical Congress trying to enact an idea that was forced on the Executive Branch by a political alliance of long-time observers, a few key Members of Congress, and the 9/11 families. A few members of Congress understood the need to bring greater unity of effort to the intelligence community and believed that creating a DNI was a necessary first step. What emerged from the tough negotiating process was far from perfect, but it provides adequate direction and authority if backed by the necessary political will.

Without strong backing from the President in interagency disputes, the DNI can only fully manage that which he or she owns. This has contributed to the growth of ODNI.

This growth has also been prompted by the constant layering on of new DNI responsibilities, some by Congress and some by agencies anxious to shed undesirable tasks.

The Dangers of a Growing Central IC Bureaucracy

To the extent that the DNI then uses its growing bureaucracy to task the rest of the community to serve the needs of the DNI, as opposed to tasking them to work toward national priorities, its primary impact will be to add to the workload of already over-stretched professionals. Additional taskings will only limit the time available for analysts and collectors to focus on actual intelligence needs.

Instead, the pyramid should be inverted, with the DNI serving the needs of IC professionals to enable them do their jobs and meet the needs of their true consumers, the decision-makers in government. Done properly, this should not undermine the authority of the DNI as the leader of the community to ensure that each element is working effectively toward national priorities. Serving the needs of the intelligence professionals does not mean allowing them to continue to go in their own direction. It means recognizing that it is these professionals who do the actual work of intelligence and making sure they have the tools, the guidance and quality time to meet the nation’s needs.

The DNI therefore should reduce the burden of information required to be sent up to the ODNI. To some degree, data calls from the DNI have been necessary to gain an initial “situational awareness.” And gathering information on how resources are deployed across the community, as noted earlier in the budget context, can provide a solid basis for evaluating how that deployment matches up against the priorities identified by the NSC and how much overlap and duplication may be occurring. However, the DNI should make it a priority to simplify the flow of that information, automating as much as possible and minimizing the need for intelligence professionals to take extra steps to compile or analyze that information.

Designating a Separate Presidential Briefer

Finally, community management can also be strengthened if the DNI is relieved of the burden of being the President’s daily intelligence briefer. It takes a significant portion of the DNI’s time each day to become expert on all of the intelligence issues of interest to the President (a task that could be delegated to senior analysts) and significantly impairs his ability to manage the community (a role only he can adequately fulfill). Moreover, the DNI becomes more personally invested in the analysis he presents to the President, making it harder to alter the analysis as new information warrants. The DNI can continue to be the President’s senior intelligence advisor without being his or her daily briefer. Ironically, the time devoted to the “daily briefer” role was one of the very reasons the CIA Director lacked the time to fulfill his DCI responsibilities to manage the overall
IC—which led to the creation of the DNI position. Thus, what we have essentially done is recreate the same time management problem one level up.

The DNI therefore should designate someone else in the IC to conduct the daily briefings of the President, while continuing to attend on a regular, but not daily, basis.

Managing HUMINT—the Limits of Intelligence: Tempering Expectations and Effectively Allocating Resources

Intelligence is a vital enabler for national security decision-making. However, it is not a panacea; intelligence consumers need to develop more realistic expectations for what intelligence can provide.

Particularly since 9/11, there has been an almost single-minded focus on developing tactical actionable intelligence about pending attacks. The reality, however, is that this is rarely achievable. In the meantime, there has been inadequate attention paid to the value of and need for better strategic intelligence and analysis to help us understand the nature of the threats we face.

Good HUMINT is far harder to acquire than most intelligence customers might imagine. Identifying, assessing and recruiting a foreign national with the right access to provide key information that meets priority intelligence requirements requires good fortune in addition to excellent tradecraft. When policymakers expect HUMINT “on demand” the result is often reporting from assets who are either of questionable credibility or marginal value.

CIA and other HUMINT entities must continue to work to establish the right balance between the number of officers operating under official cover, which present certain recruitment opportunities and protections, and those operating under non-official cover, which can provide better access to a range of targets in certain environments. The IC has struggled for decades to develop the infrastructure to deploy more officers under non-official cover. As noted elsewhere in this chapter, recruiting individuals with actual experience in the targeted cover area, rather than focusing on trying to provide that “cover” training to intelligence officers recruited out of school or very early in their careers, should become a higher priority and could accelerate that transition.

Another problem stems from the way officers in the National Clandestine Service (NCS) are evaluated. Progress has been made in moving from what was once largely a numbers game, in which promotion was based primarily on the number of assets recruited, to a greater focus on the value of those assets. However, there is still tremendous pressure to come up with recruitments in the relatively short time that an officer is in a given duty station. Recruiting high value assets takes time and has a much lower rate of success than recruiting lower-value assets. Thus, there sometimes is still an incentive to recruit marginal agents (valets, cab drivers, bartenders) at the expense of running higher-risk, higher-value but lower-likelihood-of-success recruitment operations.
HUMINT managers must ensure that performance appraisals—as well as policymaker expectations—reflect realistic expectations concerning the time it takes to establish a cover and cultivate new agents. Case officers should be rewarded for appropriate risk-taking and trade craft in addition to actual recruitments. And, of course, recruitments must be evaluated on the value of the information they bring in.

The Need to Diversify Coverage

The intelligence community is not, and cannot be, omnipresent. Too high a percentage of intelligence resources have been locked up in Iraq, leaving CIA unable to adequately cover other areas of concern. Even if fewer resources were committed to Iraq, however, the CIA should not be expected to maintain a presence, with a stable of assets and other capabilities, in every country of the world.

The DNI therefore should ensure effective deployment of other elements of the intelligence community, particularly NSA and DIA, to achieve the broadest coverage possible in today's dynamic threat environment. In a word, we have put too many of our "intelligence" eggs in a single basket. Consistent with the "Security Diversification" paradigm discussed in Chapter 5, senior intelligence managers, like managers of diversified investment portfolios, need to spread their focus among various regions and threats in order to minimize risks and avoid coverage gaps.

Too often, the IC elements are like tourists engaged in whale watching—all clustered on one side of the boat where a whale has surfaced, with no one watching for whales to surface on the other side. The DNI therefore should bring greater discipline to the allocation of assets to avoid dangerous gaps.

With regard to terrorism, at least, this will require far broader and deeper interaction with outside experts in order to understand the full context of this struggle. This means not just terrorism experts, but everything from sociologists and anthropologists to bloggers and train-spotters.

Managing Analysis—Broadening the Scope of Analysis: What Should Policy-Makers be Asking?

There are many ways to politicize intelligence. Changing or distorting analytic products to support policy is only the most blatant. Limiting analysts to answering questions asked by policymakers—rather than encouraging them to also consider what questions policymakers should be asking—can produce one-sided analysis with a limited focus. The danger is not only that politicized intelligence is likely to be less accurate, but also that in limiting the scope of issues that analysts examine, we risk neglecting areas of looming national security importance.
Analysts therefore should be rewarded in the context of performance reviews and pay raises for anticipating the kinds of questions policymakers should be asking. In addition, Congress should be viewed as a legitimate consumer of intelligence, with the ability to ask questions of the IC. This would promote a broader scope for analysis—if only because it is likely to broaden the scope of the questions asked.

**Reinforcing the Importance of Independent Analysis**

Performance appraisals are an important management tool and can be an effective motivator if they measure the right things in the right way. They can, however, also distort behavior in ways that do not contribute to better (i.e., more accurate and independent) intelligence. For example, when candidates for Senior Executive Service are told they are more likely to get a promotion if policymakers ask for them by name, or customer satisfaction becomes key to advancement, it makes it harder for an analyst to be the bearer of bad news.

Policymaker evaluations can be a valuable tool for measuring the value of intelligence. However, policymaker assessments must be taken with a grain of salt and filtered for bias based on preferred policy outcomes. Failure to do so, particularly in the context of evaluating individuals, invites politicization of intelligence. The classic management wisdom of placing the priority on pleasing the customer carries risks when applied in the intelligence context.

Accordingly, to balance the inevitable tendency to want to deliver “good” news to the policymaker, IC leadership at all levels must constantly reinforce the importance of independent analysis that goes wherever the intelligence and good tradecraft take it. The most effective way to convey this message is to lead by example. The DNI and heads of agencies must themselves be willing bearers of inconvenient news. The NIE on Iran appears to have been a good example of doing just that.

**Enhanced Use of Trusted Information Networks**

The Follow-up Report on the DNI’s 100-Day Plan provides further insight into the vision for of using trusted information networks to improve analysis. Among other thing, the Plan focuses on technology that would allow analysts to more fully interact with their colleagues in other agencies and experts outside the IC on a real-time, ongoing basis—to share questions and ideas rather than just documents. This is essential.

Accordingly, the DNI should issue guidance which encourages the use of trusted information networks both within the IC and outside the IC, including with the national security elements of other nations at the working level and with non-governmental “experts” in a wide range of fields. 576

---

Using Performance Metrics to Measure Progress and Guide Investment Decisions

The DNI’s 500-Day Plan recognizes the imperative for measuring results but, again, is short on specifics. Terms like “continual improvement,” “more accessible”, “increased interaction”, “sufficient” plans, and “clear intent and commitment” assume that any improvement constitutes success. Given the frustrations to date, perhaps that is all that can be expected.

Accordingly, the DNI should develop detailed benchmarks against which the IC intends to measure progress. These metrics, to the greatest extent possible, should be based on output rather than input or process. Moreover, the metrics should be routinely re-evaluated to see if they actually correspond to the ultimate desired outcome: better intelligence.

For example, there are indications that metrics have been developed to allow senior managers to assess progress against key hard targets. If so, this could provide an empirical basis for resolving debates over future investments in collection systems. A more accurate and precise assessment of gaps against hard targets can inform decisions about whether the Community should continue to invest as much in national technical means as it once did, or should increase investment in human and signals intelligence.

The Workforce

Ultimately, the greatest strength of the IC, and its most valuable asset, is its people. The IC must attract, hire, and train individuals with the right skill sets and experience and provide them with the right tools and incentives. The IC needs a workforce that is more diverse in terms of cultural heritage, skills and experience as well as gender, race and religion, and includes more new hires who have already spent time overseas, are proficient in languages other than English, have work experience outside of intelligence, and have had relevant training as part of their education.

Appropriately, the DNI’s first core initiative in his plans is “Treat Diversity as a Strategic Mission Imperative.” A more diverse workforce produces better results in any place of employment but it is a particularly urgent imperative for the IC, where group think is not just counterproductive but potentially dangerous. A truly diverse workforce, for example, would include analysts with different cultural backgrounds, or who have at least traveled outside the United States, to provide insights that are difficult, if not impossible, to gain from academics alone. Similarly, as HUMINT moves into non-traditional platforms, diversity in the case officer cadre with regard to background, gender, race, and ethnicity, as well as skill sets becomes increasingly vital.

But we have known this for many years. Greater progress should have been made long ago. Six years after 9/11 and more than two years after the enactment of IRTPA, the IC is still just “developing a plan” to recruit first and second generation Americans and has a

377 500 Day Plan, p. 3.
“pilot program” to “pave the way for a standard and uniform clearance process enabling us to hire and move people where and when we need them.”

Moreover, only one of the enabling initiatives in the DNI’s plans— “Improve Recruiting, Hiring and Retention of Heritage Americans (1st and 2nd Generation Americans)” — relates directly to the core element of increasing diversity. There are no specifics in the 500 Day Plan, however, for how this will be accomplished. Other enabling initiatives, such as strengthening recruiting relationships with colleges and universities and improving foreign language capability, can also support the goal of diversity but only if that goal is clearly defined as part of the enabling initiative—which it is not in the Plan. Diversity cannot be simply a hoped-for by-product of those initiatives; they must be specifically designed with the goal of diversity in mind.

Several factors combine to undermine efforts to improve the quality of recruits and their diversity in terms of cultural heritage, skills and experience. First and foremost is the control of administrative personnel over the hiring process: human resources professionals, not operators or analysts, control the development of job descriptions and qualifications, the initial screening process, the salary structure and the administration of the process itself. Thus, formal job qualifications can often be divorced from the actual knowledge and skills required to perform intelligence tasks in the real world. The current process is also heavily weighted towards intellectual and personal conformity, with psychological screening tests weeding out people with “eccentric” personalities—even when those eccentricities may be precisely what suit them for a particular job.

Second, the hiring process is too slow: from receipt of an application, through interviews, background investigations and offers can take more than three years. Particularly during a hiring surge, bottlenecks often develop in the clearance process; hiring freezes brought about by arbitrary personnel caps also inhibit timely recruiting. During this period, applicants are expected to wait patiently. Naturally, most cannot afford to do so, and take up other career opportunities instead; most of these are lost to the intelligence community, while many of those who remain are those who were not presented with career alternatives.

Third, the process is stacked against the “second career” approach of hiring people with established track records outside of intelligence. Such people do not fit into the bureaucratically-defined “career path,” and have to be inserted into the system at mid-level, without reference to seniority within the organization.

Another major impediment to innovative and skill/experience-diverse recruiting is the prevalence of bureaucratically mandated regulation and tasking which is seen by the professionals as non-mission critical and can tend at times to penalize the most professionally zealous while rewarding those who can play the bureaucratic game. Frustration among dedicated mid-level professionals can lead to chronic job dissatisfaction, which results in the best people leaving the intelligence community just as they are becoming truly valuable assets. This is especially true for case officers required to put in “career balanc-

---

378 Follow-up Report on the 100-Day Plan, p.2.
ing" tours back at headquarters, as well as for niche specialists who are underappreciated because their particular skills do not lie along the approved career path.

Compensation is only a secondary issue to recruiting; second career and other unconventional recruits are probably not joining for money but for non-material reasons. However, once in, these people do need to be compensated in accordance with their skills. Compensation reform must be implemented in a way that allows resources to be used to reward value rather than time in grade. This is essential for retention and aids recruitment.

**Work Force Recommendations**

To make material strides in improving the IC workforce, the following additional steps should be taken:

**Adopt performance standards**—Objective criteria should be developed for measuring success in increasing diversity throughout the IC. These criteria should be developed in close consultation with those engaged in the activities being measured and should be based on results, not on plans or process. They should measure progress in each element of the IC, with particular emphasis on analysis and HUMINT.

**Establish college training programs and strengthen college recruiting efforts**—This is a worthy and long overdue objective. Congress has appropriated funds for several years to initiate analyst training for college students to give them a head start in an intelligence career. These programs at colleges and universities can also help to identify and attract the kind of diversity the IC desperately needs. These are programs with great promise that needs strong support from the DNI in order to finally move off the planning desk and into classrooms at colleges and universities.

The DNI should set a goal of establishing intelligence training and recruiting programs for college students with at least two major universities or colleges within the next three years.

**Improve mid-career recruitment**—At the same time, the IC, particularly CIA, should reexamine its traditional preference for recruiting young people right out of school and assuming they will work there for their entire careers. This is no longer practicable or wise for many reasons, including the influence of a more transient workforce generally in America. Moreover, there is a serious gap in the IC between relatively new employees and very senior employees. For example, nearly 50 percent of analysts today have 5 years or less of experience in the IC.

Instead, the community should increasingly consider recruiting individuals who are in mid-career or even nearing the end of a career elsewhere. These workers can bring specialized skills and ready-made experience that would take many years and significant resources to duplicate in the IC. Moreover, while the IC may not be able to offer the kind of competitive compensation necessary to recruit specialized skills at the outset of a
career, individuals with those skills may be more interested in serving their country in the IC for a few years later in their career or as a second career.

Hiring people later in their careers would also help address the continuing difficulty in the clandestine service with developing adequate collection platforms and case officers with the skills necessary to interact with today’s intelligence targets.

The IC therefore should establish a focused recruitment program targeting mid-career and second-career applicants with non-intelligence backgrounds. This program should develop targeted incentives and accelerated training. Finding a way to effectively integrate these mid-career or late-career employees so as to fully utilize their specialized skills will also be key to attracting and retaining them.

Adjusting security clearance procedures—Hiring a new kind of workforce requires developing a new way of clearing applicants. The current clearance criteria were established at a time when the typical CIA applicant was from mainstream America and recruited right out of school. Many had never left their state, let alone the country. Clearing someone who has spent time overseas or has family overseas is currently a lengthy and cumbersome process. Director McConnell recognizes the need to alter clearance policies and advocates a simplified clearance process combined with what he calls “lifecycle monitoring.”179 The details will be important (monitoring every keystroke by every employee, as suggested by the DNI, for example, is neither feasible nor desirable), but this is the right principle.

The DNI therefore should revise the clearance criteria and process to enable more diverse hiring in a more timely manner and strengthen the IC’s ability promptly to detect suspicious activity by employees.

**Freer Flow of People, Information, and Resources**

The government cannot reorganize every time the nature of the threat changes. Instead, organizational boxes need to become less significant, replaced by policies and technologies that permit people, information, and resources to flow far more freely between the inevitable stovepipes of bureaucracy so as to maximize deployment and agility to meet inevitable changes in missions, opportunities, and the tactics of our adversaries.

**Recommendations on Free Flow of People, Information and Resources**

The following steps should be taken to make material progress in this area:

**Performance Standards for Joint Duty Program**

The “joint duty” program, initially advocated in legislation proposed by members of the House Permanent Select Committee in early 2003, appears to finally be moving

toward implementation with the promulgation of IC Policy Guidance 601.1. This program requires employees to have an assignment outside their “home” agency in order to advance to the executive level. This will continue to need careful attention and Congress will need to ensure that the policy is being implemented fully. As we learned watching the Goldwater Nichols implementation process over many years in the military, it is not enough simply to mandate joint duty for promotion. The DNI’s 500-Day Plan reflects some of the tasks that still must be undertaken, such as expanding the number of joint duty opportunities and monitoring promotion rates. Promotion opportunities will be important motivators for employees, but will be equally essential to attracting quality individuals. The joint positions offer opportunities to perform important and rewarding work—not just punching a ticket. Joint duty assignments must attract and reward professionals who are adding significant value to the intelligence effort, not just those who know how to play the game.

Congress and the DNI therefore should work together to develop criteria for evaluating the success of the joint duty program that include not only numbers of joint duty billets created and filled but also endeavor to determine whether those billets are adding value, attracting top-level talent, and rewarding them with continued advancement.

**Re-Examination of Personnel Policies**

The IC’s Personnel policies need to be re-examined to facilitate the creation of short-term mission groups, task forces, or other teams to tackle challenges that arise quickly and cut across agency expertise and capabilities. A significant aspect of this is standardizing clearances and credentialing.

The DNI therefore should direct a review of all personnel policies that impact the free flow of employees throughout the IC and make revisions to facilitate interagency collaboration. Again, this should be done not just by administrative personnel but with significant input from the professionals engaged in analysis, collection, research and development, and other key functions of the IC.

**Enhanced Information Sharing**

Unfortunately, the weakest aspect of the DNI’s plans is in the critical area of information sharing. The Report on the initial 100-Day Plan talked about having prepared memos and established interagency groups, but there is no real evidence in that report that information sharing actually increased in any significant way. Nor is its vision for where the IC should be heading particularly inspired. The subsequently issued 500-Day Plan is similarly thin. The core initiative designed to accomplish the goal of accelerating information sharing is “Enhance Intelligence Information Sharing Policies, Processes, and Procedures.” The only solid, measurable part of the plan for this goal seems to be to
establish a single community classification guide, which will be helpful but hardly suf-

cient.380

There are serious challenges to greater information sharing within the IC and with
the wide range of intelligence consumers. Some of these are based on legitimate concerns
about protecting sources and methods, law enforcement equities, or the privacy rights
of individuals. Others, however, are a result of bureaucratic intransigence, rivalries and
engrained cultures. It will require a strong commitment from the DNI to move this ini-
tiative forward.

Moreover, these efforts should recognize that information sharing is aimed at enhancing
shared knowledge and understanding. Forcing the widespread distribution of intelligence
reports, for example, is less important than enabling analysts already over-burdened with
information to share with each other their knowledge and their gaps/questions. Again,
information sharing should be aimed at improving intelligence. Merely filling inboxes or
populating shared databases, by itself, will not accomplish that goal.

Addressing Over-Classification and its Adverse Consequences for
Information Sharing

A significant impediment to greater information sharing is the problem of over-classi-
fication. It not only prevents getting information into hands that need it. It also prevents
those potential recipients from adding their unique perspective, insight, and information
to the effort to understand the initial information.

DHS faces the most significant imperative to provide relevant information to, and
receive and analyze information from, a wide range of users who are not traditional mem-
bers of the national security community. Key players at the state and local level, in the pri-

cy sector, and within DHS’ own entities, are unlikely to have clearances. Yet they serve
vital roles in protecting the homeland and can provide, benefit from, and help analysts to
better understand, information that is gathered overseas and in the United States. If this
information is unnecessarily restricted, it threatens homeland security by hampering the
ability of these key players to contribute to the mission.

Despite the national security imperative for wide dissemination of information, virtu-
ally all of the incentives today are in favor of over-classification. The danger of not clas-
sifying information that is indeed damaging to national security is well understood. What
is not as widely appreciated is the national security risk of over-classification. Thus, there
are effectively no penalties in the system for an individual decision to classify unneces-
sarily. This will not change until performance evaluations consider classification issues.
Regular audits can provide insight into individual patterns as well as overall agency per-
formance, for example. Employees who routinely over-classify should be held accountable

380 The DNI’s Information Sharing Strategy for the United States Intelligence Community, released on February 22,
2008, again provides a useful conceptual framework and a few more specifics on next steps but is still fairly gen-
eral in its goals and calls for the development of policies and mechanisms. The IC needs to move beyond paper
writing to action.
and receive additional training. And employees should be rewarded for producing reports that can be widely disseminated. In addition, the system should make it easy to produce unclassified documents and require a bit more effort to classify something. Requiring that unclassified documents be written first and enforcing the requirement for portion marking are some examples. Requiring that the specific harm to national security be articulated in each case might be another possibility, although it is important not too make the system so cumbersome that it undermines the ability to be quick and agile when necessary. Ultimately, we want a process that makes it harder to go around the system than to use it.

Specifically, the DNI should take the following steps to reduce the problem of over-classification:

- reverse the “default” incentive to over-classify by including misuse of classification as a factor in employee evaluations;
- establish a certification process to ensure that those who have authority to classify documents are properly trained to recognize when information is truly sensitive;
- require regular audits of classified documents to assess the scope and nature of any over-classification and to provide a basis for including misuse of classification in employee evaluations;
- require that documents be written in unclassified version first, to the maximum extent possible, rather than settling for occasional tear sheets at the bottom of a report;
- enforce “portion marking;” and
- use technology to tag bits of information as they move through the system so as to add granularity to portion marking and facilitate sanitization.

*Adopt Innovative Information Sharing Approaches*

Ultimately, the key is to enhance understanding and knowledge rather than paper flow. Too much emphasis is sometimes placed on sharing documents, rather than on sharing ideas, questions, and insights gleaned from those documents. This can often be done without revealing the sensitive information in the documents.

The DNI therefore should direct agencies to develop innovative ways of sharing information without handing over documents. For example, when dealing with unclassified but sensitive information, such as business proprietary information, DHS could consider “partnership panels” where the government and business would come together in a neutral space, share information such as vulnerability assessments and threat information, so as to enhance mutual understanding and benefit from each other’s insights, but then leave the space without having handed over the documents.
Better Use of Open Source Data

Finally, the IC should make far more effective use of a wide range of open sources to not only enhance their own understanding of key issues but also to aid in producing useful products that can be widely disseminated.

The Need for a Comprehensive Review of Domestic Intelligence Threat and Authorities

The DNI's 500-Day Plan also makes reference to possible changes in Executive Order 12333, which provides overall guidance on U.S. intelligence activities, and other policies, particularly regarding domestic intelligence gathering. This kind of review may be appropriate but should not be undertaken without significant informed public discussion and debate. Moreover, it should be done only after a comprehensive review of all laws, policies, and procedures affecting intelligence gathering with respect to U.S. persons and others inside the United States as well as a comprehensive assessment of the nature and scope of the threat inside this country from international adversaries.

Reforming the Foreign Intelligence Surveillance Act (FISA)

There is considerable debate today over the future of FISA, which is the primary statute governing domestic intelligence collection. Congress is in the midst of considering changes to FISA to address the surveillance from inside the U.S. of foreign targets overseas. There is broad agreement that communications between foreign targets should not trigger the safeguards provided in FISA. The thorny issue with which Congress has been wrestling for months, however, is how to handle communications in which one end is with someone inside the United States. The 4th Amendment to the U.S. Constitution protects the communications of persons inside the United States. Traditionally, this has not prevented the intelligence community from accessing U.S.-end communications that are acquired incidentally overseas while going after a foreign target. However, with so many more Americans today engaging in so many more international communications, it is more important than ever to ensure that the government is not accessing Americans' communications without appropriate and verifiable safeguards.

The Administration also has indicated its interest in a broader overhaul of FISA to reflect changes in technology and in the nature of the national security threats. Rather than attempt to guess at what might really be needed to meet today's challenges and how these and other changes will affect our ability to protect national security and preserve Americans' privacy, Congress should take the time needed to ensure they understand the full context in which these changes are being sought. This includes an understanding of:

- the underlying problems that have prompted these proposals, particularly as these relate to current and past intelligence activities and the changing nature of the threat; and
• how these proposed new authorities, definitions, and procedures would relate to all of the other national security and law enforcement tools available to the government.

The attacks of 9/11 revealed a vulnerability at home that led to a dramatic increase in domestic intelligence activity. The priorities of the Federal Bureau of Investigation (FBI) shifted, as it was pressed to place domestic intelligence collection at the forefront rather than criminal law enforcement. But the FBI is not the only entity engaged in domestic intelligence. The Central Intelligence Agency, National Security Agency, Department of Defense, Department of Homeland Security, and state and local law enforcement are among the many entities gathering intelligence of one type or another inside the United States.

The Need to Understand and Assess the Wide Range of Piecemeal Domestic Intelligence Authorities and Efforts

Congress and the American public should understand what all of the various U.S. government agencies are doing to gather intelligence inside the United States and make informed decisions about what activities should be taking place, by whom, and with what safeguards to protect against abuse and unwarranted or unconstitutional invasions of privacy.

The threat to the homeland presents unique challenges, both to effective intelligence and to appropriate protections against unwarranted government intrusion. Unfortunately, the legal framework governing this intelligence activity has come to resemble a Rube Goldberg contraption rather than the coherent foundation we expect and need from our laws. The rules that govern domestic intelligence collection are scattered throughout the U.S. Code and a multitude of internal agency policies, guidelines, and directives, developed piecemeal over time, often adopted quickly in response to scandal or crisis and sometimes in secret.

The various legal authorities for gathering information inside the United States, including the authorities in FISA, therefore need to be considered and understood in relation to each other, not in isolation. For example, Congress needs to understand how broader FISA authority relates to the various current authorities for obtaining or reviewing records, such as national security letters, section 215 of FISA, and the physical search pen register/trap and trace authorities in FISA, and the counterparts to these in the criminal context, as well as other law enforcement tools such as grand juries and material witness statutes.

Congress should initiate a comprehensive domestic intelligence review—In short, Congress should establish a Joint Inquiry or Task Force with representation from the most relevant committees (Intelligence, Judiciary, Armed Services, Foreign Affairs,
and Homeland Security), or an independent commission, to carefully examine the nature of the threat inside the United States and the most effective strategies for countering it. Then, armed with the results of this review, the Congress and the American public can appropriately consider whether we have the appropriate institutional and legal framework for ensuring that we have the intelligence necessary to implement those strategies, with adequate safeguards and oversight.

Congress should undertake this comprehensive consideration of domestic intelligence with an eye toward the future but informed by the past and present. Until Congress fully understands precisely what has and is being done in terms of the collection and exploitation of intelligence related to activities inside the United States, by all national security agencies, it cannot wisely anticipate the needs and potential problems going forward.